IBM Security Identity Manager
Version 6.0.0.10

Database and Directory Server Schema Topics

IBM Security Identity Manager
Version 6.0.0.10

Database and Directory Server Schema Topics

Table of contents

Table list .. vii

Chapter 1. Database tables reference .. 1

Workflow tables .. 1
- PROCESS table .. 1
- PROCESSLOG table .. 4
- PROCESSDATA table .. 7
- ACTIVITY table .. 8
- WORKITEM table .. 10
- WI_PARTICIPANT table .. 12
- PASSWORD_TRANSACTION table .. 12
- PASSWORD_SYNCH table .. 13
- NEXTVALUE table .. 13
- PENDING table .. 13
- WORKFLOW_CALLBACK table .. 14
- SYNCH_POINT table .. 14
- LISTDATA table .. 15
- ACTIVITY_LOCK table .. 15

Services tables .. 16
- RESOURCE_PROVIDERS table .. 16
- REMOTE_SERVICES_REQUESTS table .. 17
- REMOTE_RESOURCES_RECONS table .. 18
- REMOTE_RESOURCES_RECON_QUERIES table 19
- MANUAL_SERVICE_RECON_ACCOUNTS table 19
- SCRIPT table .. 20

Import and export tables .. 20
- BULK_DATA_SERVICE table .. 21
- BULK_DATA_STORE table .. 21
- BULK_DATA_INDEX table .. 21
- MIGRATION_STATUS table .. 22
- I18NMESSAGES table .. 22

Post office tables .. 22
- PO_TOPIC_TABLE .. 22
- PO_NOTIFICATION_TABLE .. 23
- PO_NOTIFICATION_HTMLBODY_TABLE .. 24

Reports tables .. 24
- ENTITY_COLUMN table .. 24
- Report table .. 25
- COLUMN_REPORT table .. 25
- AUTHORIZATION_OWNERS table .. 25
- ACI table .. 26
- ACI_ROLEDNS table .. 26
- ACI_PRINCIPALS table .. 27
- ACI_PERMISSION_ATTRIBUTERIGHT table .. 27
- ACI_PERMISSION_CLASSRIGHT table .. 27
- ENTITLEMENT table .. 28
- ENTITLEMENT_PROVISIONINGPARAMS table 28
- SYNCHRONIZATION_HISTORY table .. 29
- SYNCHRONIZATION_LOCK table .. 29
- RESOURCES_SYNCHRONIZATIONS table .. 29
- CHANGELOG table .. 30
- RECONCILIATION table .. 30
- RECONCILIATION_INFO table .. 31
- SERVICE_ACCOUNT_MAPPING table .. 31
- RECERTIFIER_DETAILS_INFO table .. 31

Role assignment attribute tables .. 32
- PERSON_ROLE_ASSIGNMENT .. 32
- PERSON_ROLE_ASSIGNMENT_VALUES table 32
- ROLE_ASSIGNMENT_ATTRIBUTES table .. 33

Provisioning policy tables .. 33
- POLICY_ANALYSIS .. 33
- POLICY_ANALYSIS_ERROR .. 34
- ACCT_CHANGE .. 35
- ATTR_CHANGE .. 36
- COMPLIANCE_ALERT table .. 37

Recertification policy tables .. 38
- RECERTIFICATIONLOG table .. 38
- USERRECERT_HISTORY table .. 39
- USERRECERT_ROLE table .. 40
- USERRECERT_ACCOUNT table .. 41
- USERRECERT_GROUP table .. 42

Shared access tables .. 42
- ERCREDENTIALLEASE table .. 42
- DB_REPLICATION_CONFIG table .. 43
- SA_BULK_LOAD table .. 44
- SA_CREDPOOL_DESCRIPTION table .. 44
- SA_CREDPOOL_GROUP table .. 44
- SA_CREDPOOL_OWNER table .. 45
- SA_EVALUATION_BU table .. 45
- SA_EVALUATION_BU_HIERARCHY table .. 45
- SA_EVALUATION_CREDENTIAL table .. 46
- SA_EVAL_CRED_DESCRIPTION table .. 47
- SA_EVALUATION_CREDENTIAL_POOL table 47
- SA_EVALUATION_SERVICE table .. 48
- SA_EVALUATION_SERVICE_TAG table .. 48
- SA_GLOBAL_CONFIGURATION table .. 49
- SA_POLICY table .. 50
- SA_POLICY_DESCRIPTION table .. 51
- SA_POLICY_ENTITLEMENT table .. 51
- SA_POLICY_ERURI table .. 52
- SA_POLICY_MEMBERSHIP table .. 52
- SA_VAULT_SERVICE table .. 53
- SA_VAULT_SERVICE_ALIAS table .. 53
- SYNCH_OBJECT_LOCK table .. 54
- V_AUTHORIZED_CREDENTIALS view .. 54
- V_AUTHORIZED_CREDENTIALPOOLS view . 54
- V_SA_EVALUATION_SERVICE view .. 55
- V_SAPOLICY_ENTITLEMENT_DETAIL view .. 55

Access catalog tables and views .. 56
- T_AccessCatalog table .. 56
- T_AccessCatalogTags table .. 57
- T_BADGES table .. 58
- T_Owner table .. 58
- T_GROUP table .. 58
- T_Role table .. 59
- T_ProvisioningPolicy table .. 59
- T_PolicyMembership table .. 60
- T_ServiceEntitlement table .. 60
- T_AttributeEntitlement table .. 60
- T_ServiceTags table .. 61
- TMP_HostSEByPerson table .. 61

TMP_JSAEByPerson table .. 62
T_Global_Settings table .. 62
T_GROUP_PROFILE table .. 63
T_Joindirective table .. 63
V_GroupCatalog view .. 63
V_RoleCatalog view .. 64
V_ServiceCatalog view .. 65
V_DYNAMIC_ENTITLEMENT view .. 66
V_ServiceEntitlementByRole view .. 66
V_GROUP_PROFILE view .. 67
V_GC_INTERSECT view .. 67
V_GC_CUSTOM view .. 68
Database views tables .. 70
PENDING_APPROVAL view .. 70
ROOTPROCESSVIEW view .. 70
SUBPROCESSVIEW view .. 70
SUSPENDED_USERS view .. 71
SUSPENDED_ACCOUNT_OPERATIONS view 71
PROCESS_VIEW view .. 72
Separation of duty policy tables .. 72
SOD_OWNER table .. 72
SOD_POLICY table .. 73
SOD_RULE table .. 73
SOD_RULE_ROLE table .. 74
SOD_VIOLATION_HISTORY table .. 74
SOD_VIOLATION_STATUS table .. 75
SOD_VIOLATION_ROLE_MAP table .. 76
Others .. 76
ACI_CATEGORIES table .. 77
AUTH_KEY table .. 77
COMMON_TASKS table .. 77
LCR_INPROGRESS_TABLE table .. 77
ROLE_INHERITANCE table .. 78
SCHEDULED_MESSAGE table .. 78
TASK_TREE table .. 79
TASKS_VIEWABLE table .. 79
VIEW_DEFINITION table .. 79

Chapter 2. IBM Security Directory Server schema and class reference .. 81

IBM Security Identity Manager directory tree .. 81
General classes .. 83
erBPPersonItem .. 83
erBPOrg .. 84
erBPOrgItem .. 84
erDictionary .. 85
erDictionaryItem .. 85
erDynamicRole .. 85
erFormTemplate .. 85
erIdentityExclusion .. 86
erLocationItem .. 86
erManagedItem .. 86
erOrganizationItem .. 87
erOrgUnitItem .. 87
erPersonItem .. 87
erRole .. 89
erSecurityDomainItem .. 89
SecurityDomain .. 89
erTemplate .. 90
erTenant .. 90
erWorkflowDefinition .. 93
erOwnershipType .. 93
Service classes .. 93
erAccessItem .. 93
erAccessType .. 94
erAccountItem .. 94
erADJNDIFeed .. 96
erAttributeConstraint .. 97
erChallenges .. 97
erComplianceIssue .. 98
erCSVFeed .. 98
erDSMLInfoService .. 99
erDSML2Service .. 99
erGroupItem .. 100
erHostedAccountItem .. 100
erHostedService .. 101
erHostSelectionPolicy .. 101
erITIMService .. 101
erJNDIFeed .. 101
erJoinDirective .. 102
erPrivilegeRule .. 102
erObjectCategory .. 103
erObjectProfile .. 103
erLifecycleProfile .. 104
erRemoteServiceItem .. 104
erServiceItem .. 104
erServiceProfile .. 105
erSystemItem .. 106
erSystemRole .. 106
erSystemUser .. 106
Policy classes .. 106
erAccountTemplate .. 107
erAdoptionPolicy .. 107
erIdentityPolicy .. 107
erPasswordPolicy .. 107
erPolicyBase .. 107
erPolicyItemBase .. 108
erProvisioningPolicy .. 108
erRecertificationPolicy .. 109
erSeparationOfDutyPolicy .. 110
erSeparationOfDutyRule .. 110

Chapter 3. Auditing schema tables 113

AUDIT_EVENT table .. 114
IBM Security Identity Manager authentication .. 115
Values for columns in the AUDIT_EVENT table 115
Table columns in the AUDIT_EVENT table .. 115
Person management .. 116
AUDIT_MGMT_TARGET table .. 116
Values for columns in the AUDIT_EVENT table 116
Table columns used in the AUDIT_EVENT table 117
Table columns for person management in the AUDIT_MGMT_ACCESS_REQUEST table .. 118
Table columns for person management in the AUDIT_MGMT_OBLIGATION table .. 118
AUDIT_MGMT_OBLIGATION_ATTRIB table 118
AUDIT_MGMT_OBLIGATION_RESOURCE table .. 119
Delegate authority .. 119
AUDIT_MGMT_DELEGATE table .. 119
Values for columns in the AUDIT_EVENT table 120
Table columns used in the AUDIT_EVENT table 120

Policy management 120
Values for columns in the AUDIT_EVENT table 120
Table columns used in the AUDIT_EVENT table 121
ACI management 124
AUDIT_MGMT_TARGET table 124
Values for columns in the AUDIT_EVENT table 124
Table columns used in the AUDIT_EVENT table 125
Access request management 125
AUDIT_MGMT_ACCESS_REQUEST table. . 126
AUDIT_MGMT_OBLIGATION table. . . . 127
AUDIT_MGMT_OBLIGATION_ATTRIB table 128
AUDIT_MGMT_OBLIGATION_RESOURCE table 129
AUDIT_MGMT_MESSAGE table 129
Values for columns in the AUDIT_EVENT table that is used by access request management . . 129
Table columns used in the AUDIT_EVENT table 130
Manual activity events 130
Create manual activity event 130
Escalate manual activity event. 135
Table columns used in the AUDIT_Event table 138
Lifecycle rule events 138
Values for columns in the AUDIT_EVENT table 138
Table columns used in the AUDIT_EVENT table 139
Account management 139
AUDIT_MGMT_PROVISIONING table . . . 139
Values for columns in the AUDIT_EVENT table 140
Table columns used in the AUDIT_EVENT table 140
Table columns for account management in the AUDIT_MGMT_ACCESS_REQUEST table. . 141
Table columns for account management in the AUDIT_MGMT_OBLIGATION table. . . . 142
AUDIT_MGMT_OBLIGATION_ATTRIB table 142
AUDIT_MGMT_OBLIGATION_RESOURCE table 142
Container management 143
Values for columns in the AUDIT_EVENT table 143
Table columns used in the AUDIT_EVENT table 143
Organization role management 144
AUDIT_MGMT_TARGET table 144
Values for columns in the AUDIT_EVENT table 144
Table columns used in the AUDIT_EVENT table 145
ITIM group management 146
AUDIT_MGMT_TARGET table 146
Values for columns in the AUDIT_EVENT table 146
Table columns used in the AUDIT_EVENT table 147
Service management 147
AUDIT_MGNT_TARGET table 148
Values for columns in the AUDIT_EVENT table 148
Table columns used in the AUDIT_EVENT table 148
Group management 149
AUDIT_MGMT_TARGET table 149
Values for columns in the AUDIT_EVENT table 150
Table columns used in the AUDIT_EVENT table 150
Service policy enforcement 151
Values for columns in the AUDIT_EVENT table 151
Table columns used in the AUDIT_EVENT table 151
Reconciliation 151
Values for columns in the AUDIT_EVENT table 152
Table columns used in the AUDIT_EVENT table 152
Entitlement workflow management 152
Values for columns in the AUDIT_EVENT table 152
Table columns used in the AUDIT_EVENT table 153
Entity operation management 153
Values for columns in the AUDIT_EVENT table 153
Table columns used in the AUDIT_EVENT table 154
System configuration 154
Values for columns in the AUDIT_EVENT table 154
Table columns used in the AUDIT_EVENT table 155
Runtime events. 156
Values for columns in the AUDIT_EVENT table 156
Table columns used in the AUDIT_EVENT table 157
Self-password change 157
Values for columns in the AUDIT_EVENT table 157
Table columns used in the AUDIT_EVENT table 157
Migration 158
Values for columns in the AUDIT_EVENT table 158
Table columns used in the AUDIT_EVENT table 158
Credential management 159
Values for columns in the AUDIT_EVENT table 159
Table columns used in the AUDIT_EVENT table 159
Credential Pool management 160
Values for columns in the AUDIT_EVENT table 160
Table columns used in the AUDIT_EVENT table 160
Credential Lease management 161
AUDIT_MGMT_LEASE table 161
Values for columns in the AUDIT_EVENT table 161
Table columns used in the AUDIT_EVENT table 162

Chapter 4. IBM Cognos reporting query subjects and query items . . 165

Schema mapping 165
Mapping the attributes and entities 165
`Recertification Audit` namespace 166
Query subjects for `Recertification Audit` namespace 167
Query items for `Recertification Audit` namespace 168
`Recertification Config` namespace. 176
Query subjects for `Recertification Config` namespace 176
Query items for `Recertification Config` namespace 176
`Account Audit` namespace 183
Query subjects for `Account Audit` namespace 183
Query items for `Account Audit` namespace . . 184
`Account Configuration` namespace 187
Query subjects for `Account Configuration` namespace 187
Query items for `Account Configuration` namespace 189
`Provisioning Policy Audit` namespace. . . . 196
Query subjects for `Provisioning Policy Audit` namespace 196
Query items for `Provisioning Policy Audit` namespace 197
`Provisioning Policy Config` namespace . . . 199
Query subjects for `Provisioning Policy Config` namespace 199
Query items for `Provisioning Policy Config` namespace 200
`Role Audit` namespace 203

Query subjects for Role Audit namespace . .. 203
Query items for Role Audit namespace. . .. 204
Role Configuration namespace 206
Query subjects for Role Configuration namespace 206
Query items for Role Configuration namespace 208
Separation of Duty Audit namespace 213
Query subjects for Separation of Duty Audit namespace 213
Query items for Separation of Duty Audit namespace 214
Separation of Duty Configuration namespace .. 219
Query subjects for Separation of Duty Configuration namespace 219
Query items for Separation of Duty Configuration namespace 220
User Audit namespace 221
Query subjects for User Audit namespace . .. 221
Query items for User Audit namespace. . .. 222
User Configuration namespace 225
Query subjects for User Configuration namespace 225
Query items for User Configuration namespace 226
Service Audit namespace 233
Query subjects for Service Audit namespace 233
Query items for Service Audit namespace .. 234
Access Audit namespace 236
Query subjects for Access Audit namespace .. 237
Query items for Access Audit namespace . .. 238
Access Configuration namespace 242
Query subjects for Access Configuration namespace 242
Query items for Access Configuration namespace 243

Index 247

Table list

1. PROCESS table 1
2. PROCESSLOG table 4
3. PROCESSDATA table 7
4. ACTIVITY table 8
5. WORKITEM table 10
6. WI_PARTICIPANT table 12
7. PASSWORD_TRANSACTION table 13
8. PASSWORD_SYNCH table 13
9. NEXTVALUE table 13
10. PENDING table 14
11. WORKFLOW_CALLBACK table 14
12. SYNCH_POINT table 14
13. LISTDATA table 15
14. ACTIVITY_LOCK table 15
15. RESOURCE_PROVIDERS table 16
16. REMOTE_SERVICES_REQUESTS table 17
17. REMOTE_RESOURCES_RECONS table 18
18. REMOTE_RESOURCES_RECON_QUERIES table 19
19. MANUAL_SERVICE_RECON_ACCOUNTS table 19
20. SCRIPT table 20
21. BULK_DATA_SERVICE table 21
22. BULK_DATA_STORE table 21
23. BULK_DATA_INDEX table 21
24. MIGRATION_STATUS table 22
25. I18NMESSAGES table 22
26. PO_TOPIC_TABLE table 23
27. PO_NOTIFICATION_TABLE table 23
28. PO_NOTIFICATION_HTMLBODY_TABLE 24
29. ENTITY_COLUMN table 24
30. Report table 25
31. COLUMN_REPORT table 25
32. AUTHORIZATION_OWNERS table 26
33. ACI table 26
34. ACI_ROLEDNS table 26
35. ACI_PRINCIPALS table 27
36. ACI_PERMISSION_ATTRIBUTERIGHT table 27
37. ACI_PERMISSION_CLASSRIGHT table 27
38. ENTITLEMENT table 28
39. ENTITLEMENT_PROVISIONINGPARAMS table 28
40. SYNCHRONIZATION_HISTORY table 29
41. SYNCHRONIZATION_LOCK table 29
42. RESOURCES_SYNCHRONIZATIONS table 29
43. CHANGELOG table 30
44. RECONCILIATION table 30
45. RECONCILIATION_INFO table 31
46. SERVICE_ACCOUNT_MAPPING table 31
47. RECERTIFIER_DETAILS_INFO table 31
48. The PERSON_ROLE_ASSIGNMENT table 32
49. The PERSON_ROLE_ASSIGNMENT table 32
50. The ROLE_ASSIGNMENT_ATTRIBUTES table 33
51. POLICY_ANALYSIS table 33
52. POLICY_ANALYSIS_ERROR table 34
53. ACCT_CHANGE table 35
54. ATTR_CHANGE table 36
55. COMPLIANCE_ALERT table 37
56. RECERTIFICATIONLOG table 38
57. USERRECERT_HISTORY table 40
58. USERRECERT_ROLE table 40
59. USERRECERT_ACCOUNT table 41
60. USERRECERT_GROUP table 42
61. ERCREDENTIALLEASE table 42
62. DB_REPLICATION_CONFIG table 43
63. SA_BULK_LOAD table 44
64. SA_CREDPOOL_DESCRIPTION table 44
65. SA_CREDPOOL_GROUP table 44
66. SA_CREDPOOL_OWNER table 45
67. SA_EVALUATION_BU table 45
68. SA_EVALUATION_BU_HIERARCHY table 45
69. SA_EVALUATION_CREDENTIAL table 46
70. SA_EVAL_CRED_DESCRIPTION table 47
71. SA_ EVALUATION_CREDENTIAL_POOL table 47
72. SA_EVALUATION_SERVICE table 48
73. SA_EVALUATION_SERVICE_TAG table 49
74. The SA_GLOBAL_CONFIGURATION table 49
75. SA_POLICY table 50
76. SA_POLICY_DESCRIPTION table 51
77. SA_POLICY_ENTITLEMENT table 51
78. SA_POLICY_ERURI table 52
79. SA_POLICY_MEMBERSHIP table 52
80. SA_VAULT_SERVICE table 53
81. SA_VAULT_SERVICE_ALIAS table 53
82. SYNCH_OBJECT_LOCK table 54
83. V_AUTHORIZED_CREDENTIALS view 54
84. V_AUTHORIZED_CREDENTIALPOOLS view 54
85. V_SA_EVALUATION_SERVICE view 55
86. V_SAPOLICY_ENTITLEMENT_DETAIL view 55
87. T_AccessCatalog table 56
88. T_AccessCatalogTags table 57
89. T_BADGES table 58
90. T_Owner table 58
91. T_GROUP table 58
92. T_Role table 59
93. T_ProvisioningPolicy table 59
94. T_PolicyMembership table 60
95. T_ServiceEntitlement table 60
96. T_AttributeEntitlement table 61
97. T_ServiceTags table 61
98. TMP_HostSEByPerson table 62
99. TMP_JSAEByPerson table 62
100. T_Global_Settings table 63
101. T_GROUP_PROFILE table 63
102. T_Joindirective table 63
103. V_GroupCatalog view 63
104. V_RoleCatalog view 64
105. V_ServiceCatalog view 65
106. V_DYNAMIC_ENTITLEMENT view 66
107. V_ServiceEntitlementByRole view 66
108. V_GROUP_PROFILE view 67
109. V_GC_INTERSECT view 67
110. V_GC_CUSTOM view 69
111. PENDING_APPROVAL view 70
112. ROOTPROCESSVIEW view table 70

113. SUBPROCESSVIEW view table .. 70
114. SUSPENDED_USERS view table .. 71
115. SUSPENDED_ACCOUNT_OPERATIONS view table 72
116. PROCESS_VIEW view table .. 72
117. SOD_OWNER table .. 72
118. SOD_POLICY table .. 73
119. SOD_RULE table .. 73
120. SOD_RULE_ROLE table .. 74
121. SOD_VIOLATION_HISTORY table .. 74
122. SOD_VIOLATION_STATUS table .. 75
123. SOD_VIOLATION_ROLE_MAP table .. 76
124. ACI_CATEGORIES table .. 77
125. AUTH_KEY table .. 77
126. COMMON_TASKS table .. 77
127. LCR_INPROGRESS_TABLE table .. 77
128. ROLE_INHERITANCE table .. 78
129. SCHEDULED_MESSAGE table .. 78
130. TASK_TREE table .. 79
131. TASKS_VIEWABLE table .. 79
132. VIEW_DEFINITION table .. 79
133. Brief descriptions of each container in the directory tree .. 81
134. erBPPersonItem table .. 83
135. erBPOrg table .. 84
136. erBPOrgItem table .. 85
137. erDictionary table .. 85
138. erDictionaryItem table .. 85
139. erDynamicRole table .. 85
140. erFormTemplate table .. 86
141. erIdentityExclusion table .. 86
142. erLocationItem table .. 86
143. erManagedItem table .. 86
144. erOrganizationItem table .. 87
145. erOrgUnitItem table .. 87
146. erPersonItem table .. 88
147. erRole table .. 89
148. erSecurityDomainItem table .. 89
149. SecurityDomain table .. 90
150. erTemplate table .. 90
151. erTenant table .. 91
152. erWorkflowDefinition table .. 93
153. erOwnershipType table .. 93
154. erAccessItem table .. 94
155. erAccessType table .. 94
156. erAccountItem table .. 94
157. erADJNDIFeed table .. 96
158. erAttributeConstraint table .. 97
159. erChallenges table .. 97
160. erComplianceIssue table .. 98
161. erCSVFeed table .. 98
162. erDSMLInfoService table .. 99
163. erDSML2Service table .. 99
164. erGroupItem table .. 100
165. erHostedAccountItem table .. 100
166. erHostedService table .. 101
167. erHostSelectionPolicy table .. 101
168. erITIMService table .. 101
169. erJNDIFeed table .. 101
170. erJoinDirective table .. 102
171. erPrivilegeRule table .. 102
172. erObjectCategory table .. 103
173. erObjectProfile table .. 103
174. erLifecycleProfile table .. 104
175. erRemoteServiceItem table .. 104
176. erServiceItem table .. 104
177. erServiceProfile table .. 105
178. erSystemRole table .. 106
179. erServiceProfile table .. 106
180. erAccountTemplate table .. 107
181. erAdoptionPolicy table .. 107
182. erIdentityPolicy table .. 107
183. erPasswordPolicy table .. 107
184. erPolicyBase table .. 108
185. erPolicyItemBase table .. 108
186. erProvisioningPolicy table .. 108
187. erRecertificationPolicy table .. 109
188. erSeparationOfDutyPolicy table .. 110
189. erSeparationOfDutyPolicy table .. 110
190. Auditing schema tables .. 113
191. AUDIT_EVENT table .. 114
192. Column values in the AUDIT_EVENT table 115
193. AUDIT_MGMT_TARGET table .. 116
194. Values for columns in the AUDIT_EVENT table 116
195. **AccessRequest** values for the **AUDIT_MGMT_OBLIGATION_ATTRIB** table .. 118
196. **AccessRequest** values for the **AUDIT_MGMT_OBLIGATION_RESOURCE** table .. 119
197. AUDIT_MGMT_DELEGATE table .. 119
198. Values for columns in the AUDIT_EVENT table 120
199. Values for columns in the AUDIT_EVENT table 120
200. AUDIT_MGMT_TARGET table .. 124
201. Values for columns in the AUDIT_EVENT table 124
202. **AUDIT_MGMT_ACCESS_REQUEST** table for access request management .. 126
203. **AccessRequest** values for the **AUDIT_MGMT_OBLIGATION** table .. 127
204. **AccessRequest** values for the **AUDIT_MGMT_OBLIGATION_ATTRIB** table .. 128
205. **AccessRequest** values for the **AUDIT_MGMT_OBLIGATION_RESOURCE** table .. 129
206. **AUDIT_MGMT_MESSAGE** table for access request management .. 129
207. AUDIT_EVENT table for access request management .. 129
208. Create manual activity values for the **AUDIT_MGMT_ACTIVITY** table .. 131
209. Create manual activity values for the **AUDIT_MGMT_PARTICIPANT** table .. 134
210. AUDIT_EVENT table for the create manual activity event .. 135
211. Escalate manual activity values for the **AUDIT_MGMT_ACTIVITY** table .. 136
212. Escalate manual activity values for the **AUDIT_MGMT_ACTIVITY** table .. 136
213. Escalate manual activity event values for the **AUDIT_MGMT_PARTICIPANT** table .. 137
214. AUDIT_EVENT table for the escalate manual activity event .. 138
215. AUDIT_EVENT table for lifecycle rule events 138
216. AUDIT_MGMT_PROVISIONING table .. 139
217. Values for columns in the AUDIT_EVENT table 140

218. **AccessRequest** values for the **AUDIT_MGMT_OBLIGATION_ATTRIB** table 142
219. **AccessRequest** values for the **AUDIT_MGMT_OBLIGATION_RESOURCE** table . .. 142
220. Values for columns in the AUDIT_EVENT table 143
221. AUDIT_MGMT_TARGET table 144
222. Values for columns in the AUDIT_EVENT table 144
223. AUDIT_MGMT_TARGET table 146
224. Values for columns in the AUDIT_EVENT table 146
225. AUDIT_MGNT_TARGET table 148
226. Values for columns in the AUDIT_EVENT table 148
227. AUDIT_MGMT_TARGET table 149
228. Values for columns in the AUDIT_EVENT table 150
229. Values for columns in the AUDIT_EVENT table 151
230. Values for columns in the AUDIT_EVENT table 152
231. Values for columns in the AUDIT_EVENT table 152
232. Values for columns in the AUDIT_EVENT table 153
233. Values for columns in the AUDIT_EVENT table 154
234. Value of the entity_name column table 155
235. Values for columns in the AUDIT_EVENT table 156
236. Values for columns in the AUDIT_EVENT table 157
237. Values for columns in the AUDIT_EVENT table 158
238. Values for columns in the AUDIT_EVENT table 159
239. Values for columns in the AUDIT_EVENT table 160
240. AUDIT_MGMT_LEASE table 161
241. Values for columns in the AUDIT_EVENT table 161
242. Mapping the attributes and entities 165
243. Query subjects in the Recertification Audit namespace for the recertification model . .. 167
244. Query items in the Recertification Audit namespace 168
245. Query subjects in the Recertification Config namespace 176
246. List of query items in the Recertification Config namespace 177
247. Query subjects in the Account Audit namespace 183
248. Query items in the Account Audit namespace 184
249. Query subjects in the Account Configuration namespace 187
250. Query items in the Account Configuration namespace 189
251. Query subjects in the Provisioning Policy Audit namespace 196
252. Query items in the Provisioning Policy Audit namespace 198
253. Query subjects in the Provisioning Policy Config namespace 200
254. Query items in the Provisioning Policy Config namespace 201
255. Query subjects in the Role Audit namespace 203
256. List of query items in the Role Audit namespace 204
257. Query subjects in the Role Configuration namespace 206
258. List of query items in the Role Configuration namespace 208
259. Query subjects in the Separation of Duty Audit namespace 214
260. Query items in the Separation of Duty Audit namespace 215
261. Query subjects in the Separation of Duty Configuration namespace 219
262. Query items in the Separation of Duty Configuration namespace 220
263. Query subjects in the User Audit namespace 221
264. List of query items in the User Audit namespace 222
265. Query subjects in the User Configuration namespace 225
266. List of query items in the User Configuration namespace 226
267. Query subjects in the Service Audit namespace 233
268. List of query items in the Service Audit namespace 234
269. Query subjects in the Access Audit namespace 237
270. List of query items in the Access Audit namespace 238
271. Query subjects in the Access Configuration namespace 242
272. List of query items in the Access Configuration namespace 243

Chapter 1. Database tables reference

IBM® Security Identity Manager loads the database tables during installation. The loaded tables are described in this section.

Workflow tables

IBM Security Identity Manager stores workflow-specific information in the database tables described in this section.

The workflow engine accesses these tables to retrieve information that is used during the workflow process.

PROCESS table

The PROCESS table stores all the pending, running, and historical requests submitted to the IBM Security Identity Manager workflow. Each request is represented as a process.

Table 1. PROCESS table

Column Name	Description	Data type
ROOT_PROCESS_ID*	The root process ID number.	Numeric
ID*	Process ID number. Primary key.	Numeric
PARENT_ID	Parent process ID number, if any.	Numeric
PARENT_ACTIVITY_ID	Parent activity ID number.	Numeric
NAME	Process name.	Character (100)

Table 1. PROCESS table (continued)

Column Name	Description	Data type
TYPE*	Process type code. Values include: • Access Request Batch Processing (AB) • User Data Change (UC) • User BU Change (UO) • Suspend User (US) • Restore User (UR) • Delete User (UD) • New User (UA) • Suspend Multiple Users (MS) • Restore Multiple Users (MR) • Delete Multiple Users (MD) • Account Add (AA) • Account Change (AC) • Account Password Change (AP) • Suspend Multiple Accounts (LS) • Restore Multiple Accounts (LR) • Delete Multiple Accounts (LD) • Change Password for Multiple Accounts (LP) • Suspend Account (AS) • Restore Account (AR) • Delete Account (AD) • Reconciliation (RC) • Add Provisioning Policy (PA) • Modify Provisioning Policy (PC) • Delete Provisioning Policy (PD) • Add Service Selection Policy (SA) • Modify Service Selection Policy (SC) • Delete Service Selection Policy (SD) • Add Dynamic Role (DA) • Modify Dynamic Role (DC) • Remove Dynamic Role (DD) • Account Add (OA) • Account Modify (OC) • Provision Ordered Accounts (OP) • Self-Register Person Operation (SR) • Multi Account Adopt Operation (LO) • Account Adopt Operation (AO) • Policy Enforcement for Service (PS) • Policy Enforcement for Account (EN) • Import or Export Policy Enforcement (PE) • Life Cycle Rule Execution (LC) • Custom Process (CP) • Entitlement Process (EP) • Recertification Policy (RP)[1] • Manual Service (SM)[1] • Multiple Account State Change (MA)[1] • Access Entitlement Request (EA)[1] • Access Entitlement Removal (ER)[1] • Human Resource Feed (HR)[1] • Add Separation of Duty Policy (SP)[2] • Delete Separation of Duty Policy (SX)[2] • Modify Separation of Duty Policy (SU)[2] • Evaluate Separation of Duty Policy (DR)[2] • Separation of Duty Policy Violation Evaluation (DE)[2] • Separation of Duty Policy Violation Approval (DP)[2] • Change Role Hierarchy (CR)[2] • Add Credential to Vault (VA)[3] • Check in (CI)[3] • Check out (CO)[3] • Handle an Expired Lease (EL)[3] • Process all Expired Leases (PL)[3] • Bulk Load Shared Accesses (BL)[3] • Enforce Policies for Service (SE)[3] • Connect credential to account (CC)[4]	Character (2)
DEFINITION_ID*	Process definition identifier.	Character (2000)

Table 1. PROCESS table (continued)

Column Name	Description	Data type
REQUESTER_TYPE	Requester type. Values include: • End User (U) • Workflow System (S) • Tenant Administrator (T) • Security Identity Manager System (P)	Character (2)
REQUESTER	DN of the requester.	Character (2000)
REQUESTER_NAME	Requesters name.	Character (100)
DESCRIPTION	Description of the process.	Character (300)
PRIORITY	Priority of the process.	Numeric
SCHEDULED	Scheduled start time for the process.	Character (50)
STARTED	Time that the process is started.	Character (50)
COMPLETED	Time that the process is completed.	Character (50)
LASTMODIFIED	Time that the process was last modified.	Character (50)
SUBMITTED	Time that the process was submitted.	Character (50)
STATE	Current state of the process. Values include: • Running (R) • Not Started (I) • Terminated (T) • Aborted (A) • Suspended (S) • Completed (C) • Bypassed (B)	Character (1)
NOTIFY	Specifies who is notified when a process is completed. You have the following choices: • NOTIFY_NONE (0) • NOTIFY_REQUESTOR (1) • NOTIFY_REQUESTEDFOR (2) • NOTIFY_BOTH (3)	Numeric
REQUESTEE	DN of the requestee.	Character (2000)
REQUESTEE_NAME	Name of the requestee.	Character (100)
SUBJECT	The subject of the process.	Character (2000)
SUBJECT_PROFILE	The data service object profile name that indicates the type of the subject.	Character (100)
SUBJECT_SERVICE	If the subject is an account, this field contains the name of the service associated with the account.	Character (100)
SUBJECT_ACCESS_ID[1]	DN of the requested access.	Character (2000)
SUBJECT_ACCESS_NAME[1]	Name of the requested access.	Character (100)
COMMENTS	Comments for the process.	Character (200)
RESULT_SUMMARY	Process result summary code. Values include: • Approved (AA) • Rejected (AR) • Submitted (RS) • Success (SS) • Timeout (ST) • Failed (SF) • Warning (SW) • Pending (PE) • Participant Resolution Failed (PF) • Escalated (ES) • Skipped (SK)	Character (2)
RESULT_DETAIL	Detailed information about the process result.	Long Character
SHORT_DETAIL[1]	Short detailed information about the process result.	Character (4000)
TENANT	DN of the requesters tenant.	Character (2000)

[*] Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

[2] Indicates the column or the value is added in release 5.1.

[3] Indicates the column or the value is added in release 6.0.

[4] Indicates the column or the value is added in release 6.0 Service Stream Enhancement.

PROCESSLOG table

The PROCESSLOG table maintains a record of audit events associated with a process.

Table 2. PROCESSLOG table

Column Name	Description	Data type
ID*	Log ID number. Primary key.	Numeric
PROCESS_ID	ID of the process associated with the log. Reference PROCESS (ID).	Numeric
ACTIVITY_ID	ID of the activity associated with the log.	Numeric
CREATED	Time that the log was created.	Character (50)
EVENTTYPE*	Log event type code. Values include: Activity Created (AC) Process State Changed (PS) Old Value (OV) Mail Notification (MN) Process Initial Data (PI) Process User Changed Data (PC) Process Timeout (PT) Process Escalation Participant Resolution Failed (PP) Activity Timeout (AT) Activity Escalation Timeout (AE) Activity State Changed (AS) Activity Data (AD) Activity Assignment Changed (AA) Manual Activity Performed By (CM) Activity Participant Resolution Failed (AP) Activity Escalation Participant Resolution Failed (AX) Password Pickup (PD) Message Log Information (IF)	Character (2)

Table 2. PROCESSLOG table (continued)

Column Name	Description	Data type
OLD_PARTICIPANT_TYPE	Old participant type for the assignment change event. Values include: User (U) Person (P) Role (R) System Administrator (SA) Supervisor (SU) Sponsor (SP) Service Owner (SO) System (WS) Requestor (RR) Requestee (RE) Domain Administrator (DA) Custom Defined Participant (CM) Access Owner (AO) Role Owner (RO) ITIM Group (SR)	Character (2)
OLD_PARTICIPANT_ID	Old participant ID for the assignment change event.	Character (2000)

Table 2. PROCESSLOG table (continued)

Column Name	Description	Data type
NEW_PARTICIPANT_TYPE	New participant type for the assignment change event. Values include: User (U) Person (P) Role (R) System Administrator (SA) Supervisor (SU) Sponsor (SP) Service Owner (SO) System (WS) Requestor (RR) Requestee (RE) Domain Administrator (DA) Custom Defined Participant (CM) Access Owner (AO) Role Owner (RO) ITIM Group (SR)	Character (2)
NEW_PARTICIPANT_ID	New participant ID for the assignment change event.	Character (2000)
REQUESTOR_TYPE	Requester type for any user-related event. Values include: End User (U) Workflow System (S) Tenant Administrator (T) Security Identity Manager System (P)	Character (2)
REQUESTOR	Requester name for any user-related event.	Character (2000)
REQUESTOR_DN	The DN of theSecurity Identity Manager Service account requester for any user-related event.	Character (1000)

Table 2. PROCESSLOG table (continued)

Column Name	Description	Data type
OLD_STATE	Old state for a state change event. Values include: Running (R) Not Started (I) Terminated (T) Aborted (A) Suspended (S) Completed (C) Bypassed (B)	Character (1)
NEW_STATE	New state for a state change event. Values include: Running (R) Terminated (T) Aborted (A) Suspended (S) Completed (C) Bypassed (B)	Character (1)
DATA_ID	Data ID for a data change event.	Character (100)
NEW_DATA	Data value for a data change event.	Long Character
SMALL_NEW_DATA[1]	Small data value a data change event.	Character (4000)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

PROCESSDATA table

The PROCESSDATA table stores the runtime process data of a process. After the process is completed, the record is removed.

Table 3. PROCESSDATA table

Column Name	Description	Data type
PROCESS_ID*	Process ID associated with the data. Primary key. Reference PROCESS (ID).	Numeric
DEF_ID*	Definition ID for the corresponding relevant data in the process definition. Primary key.	Character (100)
NAME	Data name. Maximum of 100 characters.	Character (100)

Table 3. PROCESSDATA table (continued)

Column Name	Description	Data type
CONTEXT	Context of data. The following values are possible : REQUESTEE SUBJECT BOTH	Character (100)
DESCRIPTION	Data description.	Character (300)
TYPE	Data type.	Character (500)
COLLECTION_TYPE	Element data type for sets of data.	Character (500)
VALUE	Data value.	Long Character
SMALL_VALUE	Small data value.	Character (4000)
VALUE_LAST_MODIFIED	The time in milliseconds that the last time this process data value was modified.	Numeric

* Indicates the column is required and not null.

ACTIVITY table

The ACTIVITY table contains records of each workflow process implementation flow.

Table 4. ACTIVITY table

Column Name	Description	Data type
ID*	Activity ID number. Primary key.	Numeric
PROCESS_ID*	Activity process ID number. Reference PROCESS (ID).	Numeric
DEFINITION_ID*	Activity definition identifier.	Character (100)
ACTIVITY_INDEX	Activity index (only if the activity is inside of a loop).	Numeric
LOOP_COUNT	Specific to loop activity. Number of iterations that occurred in the loop.	Numeric
LOOP_RUNCOUNT	Specific to asynchronous loop activity. Number of remaining iterations in the loop.	Numeric
RETRY_COUNT	Number of attempts to complete the activity.	Numeric
LOCK_COUNT	Number of pending tasks on the activity.	Numeric
SUBPROCESS_ID	ID of the subprocess associated with the activity.	Numeric
NAME	Activity name. Maximum of 100 characters.	Character (100)
DESCRIPTION	Description of the activity. Maximum of 300 characters.	Character (300)

Table 4. ACTIVITY table (continued)

Column Name	Description	Data type
TYPE	Activity type. Values include: Application (A) Subprocess (S) Loop (L) Route (R) Manual (M) Operation (O)	Character (1)
SUBTYPE	Activity subtype. Values for manual activity type include: Approval/Reject (AP) Provide Information (RI) Work Order (WO) Other activity types do not have subtype values.	Character (2)
PRIORITY	Priority of the activity (NOT SUPPORTED).	Numeric
STARTED	Time that the activity is started.	Character (50)
COMPLETED	Time that the activity is completed.	Character (50)
LASTMODIFIED	Time that the activity was last modified.	Character (50)
STATE	Current® state of the activity. Values include: Running (R) Not Started (I) Terminated (T) Canceled (A) Suspended (S) Completed (C) Bypassed (B)	Character (1)

Table 4. ACTIVITY table (continued)

Column Name	Description	Data type
RESULT_SUMMARY	Activity result summary code. Values include: Approved (AA) Rejected (AR) Submitted (RS) Success (SS) Timeout (ST) Failed (SF) Warning (SW) Pending (PE) Participant Resolution Failed (PF) Escalated (ES) Skipped (SK) Custom – custom values added for Approval and Reject codes in Enhanced Approval activities	Character (5)
RESULT_DETAIL	Detailed results information for the activity.	Long Character
SHORT_DETAIL[1]	Short detailed results information for the activity.	Character (4000)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

WORKITEM table

The WORKITEM table maintains a record of work items associated with manual workflow activities for running processes. The records associated with the process are removed after the process is completed.

Table 5. WORKITEM table

Column Name	Description	Data type
ID*	Unique work item ID. Primary key.	Numeric
PROCESS_ID*	Process ID associated with this work item. References PROCESS (ID).	Numeric
ACTIVITY_ID*	Activity ID associated with this work item. References ACTIVITY (ID).	Numeric
CREATED	Date the work item was created.	Character (50)
INPUT_PARAMETERS	Parameters that were passed into the workflow for this work item (serialized form of a list).	Long Character

Table 5. WORKITEM table (continued)

Column Name	Description	Data type
DUE_DATE	Due date for the work item. After this time, the work item is escalated, or if it already escalated, the work item is canceled.	Numeric
LOCK_OWNER	LDAP DN for the participant that currently has this work item locked (might be null if no one owns the lock).	Character (512)
DESCRIPTION	Activity ID associated with the data, if any.	Character (4000)
PROCESS_DEFINITION_ID*	The process definition ID for the process that created this work item.	Character (512)
ACTIVITY_DEFINITION_ID*	The activity definition ID for the activity that this work item relates to.	Character (100)
ACTIVITY_TYPE	The type of the activity that this work item relates to. Values include: Application (A) Subprocess (S) Loop (L) Route (R) Manual (M) Operation (O)	Character (1)
ACTIVITY_SUBTYPE	The activity subtype that corresponds to this work item. Values for manual activity type include: Approval (AP) Request For Information (RI) Work Order (WO) Compliance Alert (CA) Packaged Approval (PA)[1]	Character (2)
ACTIVITY_NAME	The activity name that corresponds with this work item.	Character (100)
REQUESTEE_NAME	The common name of the requestee of the process that created this work item.	Character (100)
REQUESTER_NAME	The common name of the entity that requested the process that created this work item.	Character (100)
SUBJECT	The subject of the process that created this work item.	Character (2000)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.1.

WI_PARTICIPANT table

The WI_PARTICIPANT table stores information about the workflow participants for a given work item. There can be more than one participant for each work item. This data is removed from the table when the work item completes.

Table 6. WI_PARTICIPANT table

Header	Header	Header
ID*	Participant unique ID. Primary Key	Numeric
WORKITEM_ID*	Work item ID that is associated with the data. References WORKITEM (ID).	Numeric
PARTICIPANT_TYPE*	Work item participant type. Values include: User (U) Person (P) Role (R) System Administrator (SA) Supervisor (SU) Sponsor (SP) Service Owner (SO) System (WS) Requestor (RR) Requestee (RE) Domain Administrator (DA) Custom Defined Participant (CM) Access Owner (AO) Role Owner (RO) ITIM Group (SR)	Character (2)
PARTICIPANT*	LDAP DN that points to the participant.	Character (512)

[*] Indicates the column is required and not null.

PASSWORD_TRANSACTION table

The PASSWORD_TRANSACTION table is used during secure password delivery to store information. After the password is retrieved, the record is deleted from the table. If the password is never picked up, this record is deleted upon password pickup expiration.

Table 7. PASSWORD_TRANSACTION table

Column Name	Description	Data type
TRANSACTION_ID*	Transaction ID used to retrieve the password. Primary key.	Numeric
ACCOUNT_DN	Account DN for the password.	Character (2000)
CREATION_DATE	Password creation date.	Character (50)
PROCESS_ID*	ID of the workflow that started the password transaction process.	Numeric
ACTIVITY_ID*	ID of the activity that started the password transaction process.	Numeric
PASSWORD	Encrypted password value.	Character (500)

* Indicates the column is required and not null.

PASSWORD_SYNCH table

The PASSWORD_SYNCH[1] table stores the account password synchronization information.

Table 8. PASSWORD_SYNCH table

Column Name	Description	Data type
ACTIVITY_ID*	The activity ID. Primary key.	Numeric
ACCOUNT_DN	The DN of the account.	Character (512)
TIME_REQUESTED	Time that the password synchronization is requested.	Character (50)
PASSWORD	The password of the account.	Character (500)

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.0.

NEXTVALUE table

The NEXTVALUE table is used to create unique IDs for workflow tables. The NEXTVALUE table is not directly used in a workflow.

Note: This table is not in use after release 4.4.

Table 9. NEXTVALUE table

Header	Header	Header
ID	Process data ID.	Numeric
NEXT_ID	Primary key ID to be used in a process.	Numeric

PENDING table

The PENDING table stores all the provisioning requests that are being processed but not yet completed.

Table 10. PENDING table

Column Name	Description	Data type
PROCESS_ID*	Process ID number. References PROCESS (ID). Primary key.	Numeric
PERSON_DN	DN of the person for which the request was submitted.	Character (255)
SERVICE_DN	DN of the resource to which to add the account.	Character (2000)

* Indicates the column is required and not null.

WORKFLOW_CALLBACK table

The WORKFLOW_CALLBACK table is used by the workflow engine to allow for callbacks to be notified when a process completed. A callback is a JMS message object (MESSAGE_OBJECT) that is put into the workflow JMS queues to be run after the PROCESS_ID completes. This callback allows for control of the workflow to be given back to the original Orchestrator of the process. After a workflow process completes, all callbacks are notified and cleared from this table.

Table 11. WORKFLOW_CALLBACK table

Column Name	Description	Data type
ID*	Identifier for a callback. Primary key.	Numeric
PROCESS_ID*	Process identifier. References PROCESS (ID)	Numeric
MESSAGE_OBJECT*	The callback message object.	Character (2000)
EVENT_TRIGGER	Workflow state that this callback is queued. Values include: Running (R) Not Started (I) Terminated (T) Aborted (A) Suspended (S) Completed (C) Bypassed (B)	Character (1)

* Indicates the column is required and not null.

SYNCH_POINT table

The SYNCH_POINT table store data used for internal state tracking of workflows and joins that need to be synchronized. Do not modify this table outside of the IBM Security Identity Manager workflow engine.

Table 12. SYNCH_POINT table

Column Name	Description	Data type
PROCESS_ID*	Process ID this sync point is associated with. Primary key.	Numeric

Table 12. SYNCH_POINT table (continued)

Column Name	Description	Data type
DEFINITION_ID*	The activity definition ID this sync point is associated with. Primary key.	Character (100)
ACTIVITY_INDEX*	The activity index this sync point is associated with. Primary key.	Numeric
WAIT_LOCK*	The wait lock this sync point is associated with. Primary key.	Numeric
JOIN_ENABLED*	Indicates whether this sync point was activated by at least one positive path through the associated workflow.	Boolean

* Indicates the column is required and not null.

LISTDATA table

The LISTDATA table optimizes memory utilization and improves performance for IBM Security Identity Manager. This table stores large data lists. Instead of loading all data into memory, data is stored in this table and referenced by index in memory.

Table 13. LISTDATA table

Column Name	Description	Data type
DATA_ID*	Unique identifier for the data. Primary key.	Numeric
INDEX_ID*	List element index. Primary key.	Numeric
VALUE*	The serialized list element.	Long Character

* Indicates the column is required and not null.

ACTIVITY_LOCK table

The activity lock count contention point can affect the performance of certain large-scale workflows. To avoid this issue, the information in the LOCK_COUNT column of the ACTIVITY table is broken into multiple rows of the ACTIVITY_LOCK table. The ACTIVITY_LOCK[1] table tracks the completion of an activity. The server and thread identifiers control which row must be incremented; only one thread attempts to update a row in this new table at any time.

Table 14. ACTIVITY_LOCK table

Column Name	Description	Data type
PROCESS_ID*	Unique ID of a process. Primary key. References PROCESS (ID).	Numeric
ACTIVITY_ID*	Unique ID of an activity. Primary key. References ACTIVITY (ID).	Numeric
SERVER*	String identifier of the server that makes the update (cell/node/server). Primary key.	Character (255)
THREAD_ID*	Identifier of the thread (within the server) making the update. Primary key.	Numeric

Table 14. ACTIVITY_LOCK table (continued)

Column Name	Description	Data type
LOCK_COUNT	Updated value, an integer counter to track when workflows are complete; it might be positive, negative, or zero.	Numeric

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.0.

Services tables

IBM Security Identity Manager creates and uses these database tables to store information related to managed resources.

RESOURCE_PROVIDERS table

The RESOURCE_PROVIDERS table stores cross-references between resource provider IDs and stores reconciliation data for each resource provider.

Table 15. RESOURCE_PROVIDERS table

Column Name	Description	Data type
PROVIDER_ID*	Unique ID for each resource provider. Primary key. There is a one-to-one relationship between a PROVIDER_ID and a RESOURCE_DN.	Character (20)
RESOURCE_DN	DN for the managed resource for which the provider is responsible.	Character (2000)
RECON_STATUS	Indicates whether reconciliation is currently running. 0 – No reconciliation is running for this service. 1 – Reconciliation is currently running on this service.If the server is shut down abruptly during reconciliation, this flag might need to be reset to 0. Reset the flag before other reconciliation requests can be processed for the specified service.	Numeric
LAST_RECON_TIME	The time of the last reconciliation.	Date
MAX_RECON_DURATION	Timeout value, in minutes, for reconciliations. If a reconciliation request runs beyond the amount of time specified in this field, the request is terminated.	Numeric
LOCK_SERVICE	Indicates whether to lock the service during a reconciliation: 0 – Do not lock the service during reconciliation. 1 – Lock the service during reconciliation.	Numeric
REQUEST_ID	Tracks the process that locks the service.	Character (20)
CURRENT_REQUEST_COUNT	Current number of requests that are being executed.	Numeric
MAX_REQUEST_COUNT	Maximum number of concurrent requests that can be executed (or -1 = unlimited). For future use (currently null).	Numeric
LAST_RESPONSE_TIME	Timestamp of last response (to detect failed resources). For future use (currently null).	Date

Table 15. RESOURCE_PROVIDERS table (continued)

Column Name	Description	Data type
RESOURCE_STATUS	Resource status (0 = ok, 1 = failed, 2 = failed service that is being tested).	Numeric
RESTART_TIME	Timestamp of the last reconciliation started.	Date
SERVER	The ID of the WebSphere® Application Server that initiated the recon. It is used in cluster mode during WebSphere Application Server restart to decide whether a recon lock flag was left enabled due to server failure. In that case, clean up locks and set the recon state to failed or aborted.	Character (255)
RESOURCE_TEST_STATUS[1]	Resource status, including updates that resulted from 'Test'(ping) request (0 = OK, 1 = failed, 2 = failed service that is being tested).	Numeric
LAST_TEST_STATUS_TIME[1]	Timestamp of last ping of the resource (to detect failed resources).	Date
FIRST_RESOURCE_FAIL_TIME[2]	Timestamp of the time the service was placed in failed state.	Timestamp
LAST_ERROR[2]	The most recent error message returned when attempting to send a request to the service.	Character (2000)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

[2] Indicates the column or the value is added in IBM Security Identity Manager release 6.0.

REMOTE_SERVICES_REQUESTS table

The REMOTE_SERVICES_REQUESTS table stores asynchronous requests or requests that are made while reconciliation is in progress. It also stores requests issued while a resource is in a failed state.

Table 16. REMOTE_SERVICES_REQUESTS table

Column Name	Description	Data type
PROVIDER_ID	Unique ID for each resource provider. References RESOURCE, PROVIDERS, and (PROVIDER_ID).	Character (20)
REQUEST_ID*	ID of the request made. Primary key.	Character (20)
TYPE	Request type: 0 – generic requests 1 – asynchronous requests 2 – intra-reconciliation requests 3 – service deferred requests	Numeric

Table 16. REMOTE_SERVICES_REQUESTS table (continued)

Column Name	Description	Data type
OPERATION	Type of operation: 0 – No operation 1 – Add request 2 – Modify request 3 – Delete request 4 – Suspend request 5 – Restore request 6 – Change password request	Numeric
REQUEST_TIME	Time that the request was made.	Date
EXPIRATION_TIME	Time that the request expires. If null, the request never expires.	Date
TARGET	The owner of the account for an add request or the account distinguished name for other types of operations.	Character (2000)
SERVICE_DN*	The distinguished name of the service instance in the directory.	Character (2000)
DATA	The data for the request (attribute values for Add and Modify requests). This information is a serialized Java™ Collection and is Base64 encoded and GZIP compressed.	Long Character
CONNECTION_POINT	The callback to complete the workflow process. This information is a serialized Java object.	Binary

* Indicates the column is required and not null.

REMOTE_RESOURCES_RECONS table

The REMOTE_RESOURCES_RECONS table stores the reconciliation units associated with a resource provider.

Table 17. REMOTE_RESOURCES_RECONS table

Column Name	Description	Data type
PROVIDER_ID*	Unique ID for each resource provider. References RESOURCE_PROVIDERS (PROVIDER_ID). Primary key.	Character (20)
RECON_ID*	Unique ID for each reconciliation unit. Primary key.	Numeric
DAY_OF_MONTH	Day of month the reconciliation is scheduled to run.	Numeric
MONTH_NUM	Month the reconciliation is scheduled to run.	Numeric
DAY_OF_WEEK	Day of week the reconciliation is scheduled to run.	Numeric
HOUR_NUM	Hour of day the reconciliation is scheduled to run.	Numeric
MINUTE_NUM	Minute of hour the reconciliation is scheduled to run.	Numeric
MAX_DURATION	This value overrides the MAX_RECON_DURATION value in the table.	Numeric

Table 17. REMOTE_RESOURCES_RECONS table (continued)

Column Name	Description	Data type
LOCK_SERVICE	Indicates whether to lock the service during a reconciliation. Values include: 0 – Do not lock the service during reconciliation. 1 – Lock the service during reconciliation Default: 1	Numeric
RECON_NAME[1]	Name of the reconciliation.	Character (300)
DESCRIPTION[1]	Description of the reconciliation.	Character (300)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

REMOTE_RESOURCES_RECON_QUERIES table

The REMOTE_RESOURCES_RECON_QUERIES table stores reconciliation queries associated with a reconciliation unit.

Table 18. REMOTE_RESOURCES_RECON_QUERIES table

Column Name	Description	Data type
PROVIDER_ID*	Unique ID for each resource provider. References REMOTE_RESOURCES_RECONS (PROVIDER_ID). Primary key.	Character (20)
RECON_ID*	Unique ID for each reconciliation unit. References REMOTE_RESOURCES_RECONS (RECON_ID). Primary key.	Numeric
QUERY_ID*	Unique ID for each reconciliation query. Primary key.	Numeric
RECON_FILTER	Filter associated with the reconciliation query.	Character (4000)
RECON_BASE	Search base associated with the reconciliation query.	Character (4000)
MAX_DURATION	Not used.	Numeric
MAX_ENTRIES	Not used.	Numeric
ATTRIBUTES	Attributes returned during a reconciliation request.	Long Character
SUPPORT_DATA_ONLY[1]	Indication whether reconciliation only retrieves supporting data. (0/null = normal, 1 = supporting data only recon).	Numeric

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

MANUAL_SERVICE_RECON_ACCOUNTS table

The MANUAL_SERVICE_RECON_ACCOUNTS[1] table stores account information for manual service. The information verifies whether the account data was modified in reconciliation.

Table 19. MANUAL_SERVICE_RECON_ACCOUNTS table

Column Name	Description	Data type
GLOBAL_ID*	Unique ID of the manual service reconciliation. Primary key.	Character (255)

Table 19. MANUAL_SERVICE_RECON_ACCOUNTS table (continued)

Column Name	Description	Data type
ACCOUNTS	The stream of the Comma Separated Value (CSV) file of last reconciliation.	Long Character

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

SCRIPT table

The SCRIPT[1] table stores predefined script rule parameters. Each row represents one parameter of a rule. A rule might consist of several rows that represent multiple attributes from the person schema to be concatenated. For example, the predefined rule, firstinitial+lastname, is a concatenation of two person attributes: givenname and sn.

Table 20. SCRIPT table

Column Name	Description	Data type
TYPE*	A character that represents the type of policy to which this rule is applied. Primary key. Values include: A – Adoption rule I – Identity policy	Character (1)
ID*	Unique identifier (key) of the rule. Primary key.	Character (50)
JOIN_ORDER*	A number that represents the order for the attribute in concatenation. Primary key.	Numeric
PERSON_ATTRIBUTE*	The person attribute where the value is obtained and concatenated; for example, givenname.	Character (100)
FIRST_LAST	A number that is used to get the substring of the person attribute. Values include: 0 – Use the whole value. -n (minus n) – Use the last n characters. n – Use the first n characters.	Numeric
CONCATENATE_CHAR	Concatenation character, which concatenates person attributes.	Character (10)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

Import and export tables

The tables in this section are used for import and export operations.

BULK_DATA_SERVICE table

The BULK_DATA_SERVICE table holds information of the export.

Table 21. BULK_DATA_SERVICE table

Column Name	Description	Data type
ID*	Unique ID of the export. Primary key.	Numeric
STARTTIME	Start time of the export.	Date
ENDTIME	End time of the export.	Date
MIMETYPE	Content type of export JAR file.	Character (50)
NAME	Name of the export JAR file.	Character (50)
DATA	Export JAR file stored in form of bytes.	Binary
FILENAME[1]	Name of export JAR file.	Character (255)
Filesize	Size of export JAR file.	Numeric
DESCNAME[1]	Description of the export.	Character (255)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

BULK_DATA_STORE table

The BULK_DATA_STORE table stores the XML content of export.

Table 22. BULK_DATA_STORE table

Column Name	Description	Data type
ID*	Unique ID for XML content of the export. Primary key.	Numeric
SERVICEID*	Unique ID of the export. References BULK_DATA_SERVICE (ID).	Numeric
XML	Content of the export XML file.	Binary

* Indicates the column is required and not null.

BULK_DATA_INDEX table

The BULK_DATA_INDEX table stores index for the data object and export XML content.

Table 23. BULK_DATA_INDEX table

Column Name	Description	Data type
ID*	Unique ID of the index for export data lookup. Primary key.	Numeric
STOREID*	ID of the export XML content. References BULK_DATA_STORE (ID).	Numeric
DATAOBJECTID	ID of the export data object.	Character (10)

* Indicates the column is required and not null.

MIGRATION_STATUS table

The MIGRATION_STATUS table stores the status of the current operation in progress.

Table 24. MIGRATION_STATUS table

Column Name	Description	Data type
ID*	Identifier generated at the beginning of an operation. The MigrationManagerBean uses it to update the status periodically. Primary key.	Numeric
PROCESSCOUNT	The number of objects processed.	Numeric
PROCESSSTATUS	The final status of the operation. This row is deleted on completion of the import/export process.	Character (50)
SERVICEID[1]	ID of the export. References BULK_DATA_SERVICE (ID).	Numeric

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

I18NMESSAGES table

The I18NMESSAGES table maintains labels in the database that allows any resource bundles to be stored.

Table 25. I18NMESSAGES table

Column Name	Description	Data type
PROFILE	Profile for which this label was inserted into the database.	Character (256)
NAME*	Contains the full name of the resource bundle, For example, the base name, country codes, and variants.	Character (256)
MESSAGEKEY*	Key that can retrieve the label.	Character (256)
MESSAGE	The label that needs to be shown to the user.	Character (2000)

* Indicates the column is required and not null.

Post office tables

The tables in this section are used by the post office function.

PO_TOPIC_TABLE

The PO_TOPIC_TABLE table stores information about the topics that are used by the post office component. There is a row in the table for each group e-mail topic that is actively in use for the system. PO_TOPIC_TABLE tracks the unique system notification email topics seen during a Post Office interval. Intercepted emails are later aggregated and forwarded on a per-topic basis.

Table 26. PO_TOPIC_TABLE table

Column Name	Description	Data type
TENANT*	The name of the tenant for which this topic applies. Primary key.	Character (256)
TOPIC*	The string that represents the group e-mail topicas defined in the notification section of the workflow definition for each manual activity. Primary key.	Character (256)
SERVER	The server that is currently processing the topic	Character (255)
CHECKPOINT_TIME	A value that represents when the current processing of this topic was started, which is the number of milliseconds since January 1, 1970, 00:00:00 Greenwich mean time.	Numeric
TOPIC_ID*	A unique ID that identifies this topic. This column keys into the PO_NOTIFICATION_TABLE to determine which messages match the topic.	Numeric

* Indicates the column is required and not null.

PO_NOTIFICATION_TABLE

The PO_NOTIFICATION_TABLE table stores information about the original notification objects that the post office component aggregates. All information about the original notification is stored in this table except for the XHTML body.

Table 27. PO_NOTIFICATION_TABLE table

Column Name	Description	Data type
NOTIFICATION_ID*	A unique ID that identifies this particular notification. Primary key.	Numeric
TOPIC_ID*	A reference to the topic ID as stored in the PO_TOPIC_TABLE for this notification. References PO_TOPIC_TABLE(TOPIC_ID).	Numeric
SUBJECT	The subject of the original notification message.	Character (2000)
TEXTBODY	The text body of the original notification message.	Long Character
RECEIVE_TIME*	The time the notification was intercepted by post office, which is the number of milliseconds since January 1, 1970, 00:00:00 Greenwich mean time.	Numeric
RECIPIENT_EADDR*	The email address of the recipient of the original notification message.	Character (320)
RECIPIENT_LOCALE	The locale of the recipient of the original notification message.	Character (256)

* Indicates the column is required and not null.

PO_NOTIFICATION_HTMLBODY_TABLE

The PO_NOTIFICATION_HTMLBODY_TABLE table stores the XHTML body of the original notification object that the post office component aggregates. All other information about the notification is stored in the PO_NOTIFICATION_TABLE table.

Table 28. PO_NOTIFICATION_HTMLBODY_TABLE

Column Name	Description	Data type
NOTIFICATION_ID*	A unique ID that identifies this particular notification (this ID is the same value that exists in the PO_NOTIFICATION_TABLE table. References PO_NOTIFICATION_TABLE(NOTIFICATION_ID). Primary key.	Numeric
HTMLBODY	The XHTML body of the original notification message that post office intercepted.	Long Character

* Indicates the column is required and not null.

Reports tables

The tables in this section are used for reporting.

ENTITY_COLUMN table

During the configuration of the IBM Security Access Manager reporting interface schema, the system administrator selects the entities and a set of attributes. The reporting Interface stores the selected pairs of entities and attributes in this table. The Report Designer can later choose to report on any of the attributes in the ENTITY_COLUMN table.

Table 29. ENTITY_COLUMN table

Column Name	Description	Data type
ENTITY_NAME*	Name of the entity (for example Person). Primary key.	Character (255)
COLUMN_NAME*	Column name as present in the entity table represented by the preceding entity name.	Character (255)
ATTRIBUTE_NAME*	Name of the attribute as returned by the IBM Security Identity Manager server. Primary key.	Character (255)
MULTI_VALUED	Indicates whether the attribute is multi-valued or not. Value is Y/N. Maximum of 1 character.	Character (1)
IMPLICITLY_MAPPED	Indicates whether the data synchronizer implicitly maps a particular attribute. If the attribute is present in the object filter of some ACI, it is implicitly mapped. Maximum of 1 character.	Character (1)
AVAILABLE_FOR_REPORTING	Indicates whether the column is available for reporting. The value for this column represents different states in which the corresponding data can be, such as newly mapped or available.	Character (255)
TABLE_NAME	Name of the table created for an entity. **Note:** V_ENTITY is a view. It is not a table.	Character (255)

* Indicates the column is required and not null.

Report table

This table stores details of the reports designed and generated by IBM Security Identity Manager users.

Table 30. Report table

Column Name	Description	Data type
ID*	Unique ID for the table. Primary key.	Numeric
TITLE*	Report title given to the report.	Character (255)
TYPE*	Indicates whether the report was designed with Security Identity Manager or RI.	Character (255)
AUTHOR	Author of the report (designer).	Character (255)
REPORT_SIZE	The size of the report template stored in the REPORT_DATA column of this table.	Numeric
REPORT_DATA	The report (custom/third party) template is stored here. The templates must be shared by the different Security Identity Manager installations in a clustered environment and so they are stored here.	Binary
STYLESHEET	Name of the style sheet for the report.	Character (255)
REPORTSUBTYPE*	Identifies if this report is a user-defined report or an out-of-box report.	Character (1)
REPORTCATEGORY*	Identifies which category the run is to be listed on the Run Reports page.	Character (255)
EDITABLE	Indicates whether this report can be edited or not. The value is N for reconciliation statistics, Audit Events, Recertification History, Pending Recertification, Recertification Policies, and access control information reports.	Character (1)

* Indicates the column is required and not null.

COLUMN_REPORT table

This table stores the relationship between the ENTITY_COLUMN table and the REPORT table. This relationship is required. It determines the reports that are affected if the system administrator changes the IBM Security Identity Manager reporting interface schema (deleting attributes available for reporting).

Table 31. COLUMN_REPORT table

Column Name	Description	Data type
COLUMN_NAME*	Name of the entity used in the report. Primary key.	Character (255)
ENTITY_NAME*	Name of the column used in the report. Primary key.	Character (255)
REPORT_ID*	ID of a report. Primary key.	Numeric

* Indicates the column is required and not null.

AUTHORIZATION_OWNERS table

This table is used for ACI Report. When a non-admin system user tries to run ACI report, it is checked whether the user is part of an authorization owner group. Custom reports can also be generated on this table.

Table 32. AUTHORIZATION_OWNERS table

Column Name	Description	Data type
USERDN*	The DN of the system user included in an authorization owner ITIM group. Primary key.	Character (255)
CONTAINERDN*	DN of the organizational container where the system user is authorized to access/modify ACI information. Primary key.	Character (255)

* Indicates the column is required and not null.

ACI table

This table stores information of the access control information items in IBM Security Identity Manager.

Table 33. ACI table

Column Name	Description	Data type
DN*	The DN of the organizational container where the ACI is defined. Primary key.	Character (255)
NAME*	Name of the ACI. Primary key.	Character (255)
SCOPE	Scope of the ACI, for example, single or subtree.	Character (255)
TARGET*	Target of this ACI. For a person ACI, the target is inetOrgPerson. Primary key.	Character (255)
PARENT	DN of the container that is the parent of this container (where the ACI is defined).	Character (255)
CATEGORY	DN of the container that is the parent of this container (where the ACI is defined).	Character (255)
OBJECTFILTER	LDAP Filter that is part of this ACI.	Character (1023)

* Indicates the column is required and not null.

ACI_ROLEDNS table

This table stores information about the IBM Security Identity Manager access control information (ACI) and the ITIM groups that are part of them. No primary key constraints are defined for this table.

Table 34. ACI_ROLEDNS table

Column Name	Description	Data type
DN*	DN of the container where the ACI is defined.	Character (255)
NAME*	Name of the ACI.	Character (255)
TARGET*	Target of this ACI.	Character (255)
ROLEDN*	DN of the ITIM group that is part of this ACI.	Character (255)

* Indicates the column is required and not null.

ACI_PRINCIPALS table

This table stores principals for access control information (ACI). No primary key constraints are defined for this table.

Table 35. ACI_PRINCIPALS table

Column Name	Description	Data type
DN*	DN of the container where the ACI is defined.	Character (255)
NAME*	Name of the ACI.	Character (255)
TARGET*	Target of this ACI.	Character (255)
PRINCIPALNAME*	Name of the principal that is part of this ACI. Possible values are self, supervisor, sponsor, and administrator.	Character (255)

* Indicates the column is required and not null.

ACI_PERMISSION_ATTRIBUTERIGHT table

This table stores attribute permissions for ACIs. No primary key constraints are defined for this table.

Table 36. ACI_PERMISSION_ATTRIBUTERIGHT table

Header	Header	Header
DN*	DN of the container where the ACI is defined.	Character (255)
NAME*	Name of the ACI.	Character (255)
TARGET*	Target of this ACI.	Character (255)
ACTION*	Permission associated with an attribute protected by this ACI. Possible values are `grant` and `deny`.	Character (6)
OPERATION*	Specifies the operation for which the preceding permission is applicable. The values for this attribute are `r` and `w`.	Character (3)
ATTRIBUTERIGHT*	Name of the attribute that is being protected by the ACI. It can be a specific attribute or all.	Character (255)

* Indicates the column is required and not null.

ACI_PERMISSION_CLASSRIGHT table

This table stores class operation permissions for ACIs. No primary key constraints are available for this table.

Table 37. ACI_PERMISSION_CLASSRIGHT table

Column Name	Description	Data type
DN*	The DN of the container where the ACI is defined.	Character (255)
NAME*	Name of the ACI.	Character (255)
TARGET*	Target of this ACI.	Character (255)
ACTION*	Permission associated with a class right, for example: grant, deny, or none.	Character (6)
CLASSRIGHT*	The class operation for this ACI, for example: search, add, or modify.	Character (255)

* Indicates the column is required and not null.

ENTITLEMENT table

This table stores the parsed entitlements of various provisioning policies in the IBM Security Identity Manager system. This table does not have a primary key constraint.

Table 38. ENTITLEMENT table

Column Name	Description	Data type
DN*	The DN of the provisioning policy or this entitlement.	Character (255)
TYPE*	Type of the entitlement. The possible values are: 0 represents a manual entitlement. 1 represents an automatic entitlement.	Character (255)
SERVICETARGETTYPE	The service target type for this entitlement. This column can have various values that represent a service profile, a service instance, all services, or a service selection policy.	Character (255)
SERVICETARGETNAME	If the service type represents a specific service instance, then this column contains the DN of the service instance.	Character (255)
PROCESSDN	The DN of the associated workflow process, if any.	Character (255)

* Indicates the column is required and not null.

ENTITLEMENT_PROVISIONINGPARAMS table

This table stores provisioning parameters for parsed entitlements. No primary key constraints are defined for this table

Table 39. ENTITLEMENT_PROVISIONINGPARAMS table

Column Name	Description	Data type
DN*	The distinguished name of the provisioning policy or this entitlement.	Character (255)
ATTRIBUTEVALUE*	Value of service attribute parameter. This value is a provisioning parameter.	Character (4000)
NAME*	Name of the service attribute parameter. These parameters are visible under **advanced provisioning parameter list** of the entitlement in IBM Security Identity Manager user interface.	Character (255)
ENFORCEMENT	Enforcement type of this service attribute parameter. Possible values represent mandatory or optional.	Character (255)
EXPRTYPE	Expression Type for this service attribute parameter. An expression can be a constant expression or a JavaScript expression.	Character (255)
SERVICETARGETNAME	If the service type represents a specific service instance, then this column contains the DN of the service instance. If service type represents a service profile or service selection policy, then this column contains the name of the service profile.	Character (255)
SERVICE_DN	Distinguished name of the associated service, if any.	Character (255)

* Indicates the column is required and not null.

SYNCHRONIZATION_HISTORY table

This table stores the history information of all the synchronizations that occurred.

Table 40. SYNCHRONIZATION_HISTORY table

Column Name	Description	Data type
SYNC_ID*	ID for this synchronization activity. Primary key.	Numeric
REQUESTOR*	Requestor of this request.	Character (255)
REQ_TYPE	This attribute specifies the type of request. DS indicates full data synchronization. IDS indicates Incremental Synchronization.	Character (255)
REQ_NAME	Name of request. For example, Data Synchronization.	Character (255)
STATUS	Status like Started, Failure, Success, or Warning[1].	Character (255)
TENANT	Tenant DN for which synchronization is run.	Character (255)
STATUS_DETAIL	Detail string of the status.	Character (255)
SCHEDULED_TIME	Time for which this synchronization was scheduled. **Note:** This attribute is deprecated. To get data synchronization schedule information, use the RESOURCES_SYNCHRONIZATIONS table.	Numeric
SUBMITTED_TIME	Time when this request was submitted.	Numeric
STARTED_TIME*	Time when this synchronization started. Primary key.	Numeric
COMPLETED_TIME	Time when this synchronization completed.	Numeric
SERVER_NAME	Name of the IBM Security Identity Manager Server that started the synchronization.	Character (255)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

SYNCHRONIZATION_LOCK table

This table is used to avoid race condition when two IBM Security Identity Manager servers in a clustered environment start data synchronization at the same time.

Table 41. SYNCHRONIZATION_LOCK table

Column Name	Description	Data type
HOST	IBM Security Identity Manager Server that acquires the lock to start data synchronization. Primary key.	Character (255)

RESOURCES_SYNCHRONIZATIONS table

This table stores the schedule information of all the synchronization schedules.

Table 42. RESOURCES_SYNCHRONIZATIONS table

Column Name	Description	Data type
SYNC_ID*	The identifier association with the synchronization. Primary key.	Numeric
DAY_OF_MONTH*	Day of month.	Numeric
MONTH_NUM*	Month number.	Numeric
DAY_OF_WEEK*	Day of week.	Numeric

Table 42. RESOURCES_SYNCHRONIZATIONS table (continued)

Column Name	Description	Data type
HOUR_NUM*	Hour number.	Numeric
MINUTE_NUM*	Minute number.	Numeric
MAX_DURATION	Maximum time for which synchronization is run.	Numeric

* Indicates the column is required and not null.

CHANGELOG table

This table stores the last change log number processed.

Table 43. CHANGELOG table

Column Name	Description	Data type
CHANGE_NUMBER*	This attribute is an integer that stores the last change log number processed by the full or incremental data synchronization.	Numeric

* Indicates the column is required and not null.

RECONCILIATION table

This table contains the summary of the information for reconciliation on various service instances. The table contains an entry for all completed reconciliations on various service instances.

Table 44. RECONCILIATION table

Column Name	Description	Data type
RECONID*	An identifier that identifies a reconciliation uniquely. Primary key.	Character (255)
SERVICEDN*	The DN of the service for which this entry is recorded.	Character (2000)
PROCESSEDACCOUNTS*	The number of processed accounts that exists for this service instance during the last run of reconciliation.	Numeric
LOCALACCOUNTS*	Total number of new local accounts created. It does not include the newly created orphan accounts for this service.	Numeric
TIMUSERACCOUNTS*	The number of processed accounts that belongs to users in IBM Security Identity Manager.	Numeric
POLICYVIOLATIONS*	The number of policy violations found for accounts on this service during reconciliation. This value includes accounts where one or more attribute values are found to be different from the local account. Any attribute value of the account is not compliant with the governing provisioning policies. It does not include accounts where the attribute values of the local and remote accounts are the same, even if the values are noncompliant.	Numeric
STARTED*	Time when the reconciliation started.	Date
COMPLETED*	Time when the reconciliation completed.	Date
ACTIVITY_ID[1]	Unique identifier of the activity.	Numeric

* Indicates the column is required and not null.

[1] Indicates the column is added in release 4.6 Express®.

RECONCILIATION_INFO table

This table contains the details of the reconciliation on various service instances.

Table 45. RECONCILIATION_INFO table

Column Name	Description	Data type
RECONID*	An identifier that identifies a reconciliation uniquely. References RECONCILIATION(RECONID).	Character (255)
ACCOUNTID	ID of any entry (for example, an account ID in case of an account reconciliation).	Character (255)
POLICYCOMPLIANCESTATUS	Policy Compliance Status of each reconciled account.	Character (20)
USERNAME	Name of the user.	Character (255)
OPERATION	The operation for the entry of this service instance. Possible values for an account entry are NL, NO, SA, DA. These values are codes that stand for various account operations. Codes include New Local, New Orphan, Suspended Account, Deprovisioned Account.	Character (20)
REMARKS	Contains the reason for deprovisioning or suspension and the list of attributes in case of modified accounts.	Character (1000)
HANDLE[1]	Only for HR Feed service when workflow is used. The process ID of the workflow request that processed this person entry. -1 for none.	Numeric

[*] Indicates the column is required and not null.

[1] Indicates the column is added in release 4.6 Express.

SERVICE_ACCOUNT_MAPPING table

The SERVICE_ACCOUNT_MAPPING$_1$ table stores the service profile and its corresponding account profile.

Table 46. SERVICE_ACCOUNT_MAPPING table

Column Name	Description	Data type
SERVICEPROFILE*	Name of service type. Primary key.	Character (255)
ACCOUNTPROFILE*	Name of the account profile corresponding to the service type. Primary key.	Character (255)

[*] Indicates the column is required and not null.

[1] Indicates the column is added in release 4.6 Express.

RECERTIFIER_DETAILS_INFO table

The RECERTIFIER_DETAILS_INFO[1] table stores the recertifier's information of recertification policies.

Table 47. RECERTIFIER_DETAILS_INFO table

Column Name	Description	Data type
DN*	The DN of the recertification policy. Primary key.	Character (255)

Table 47. RECERTIFIER_DETAILS_INFO table (continued)

Column Name	Description	Data type
RECERTIFIER_TYPE	The recertifier type. For example, Manager.	Character (255)
RECERTIFIER_NAME	The recertifier name.	Character (255)

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

Role assignment attribute tables

The tables described in this section store assignment attribute related information.

PERSON_ROLE_ASSIGNMENT

The PERSON_ROLE_ASSIGNMENT[3] table stores the role assignment information for a person.

Table 48. The PERSON_ROLE_ASSIGNMENT table

Column name	Description	Data type
ID*	The unique ID of person role assignment. Primary key.	Numeric
PERSON_DN*	The person DN.	Character (2000)
ROLE_DEFINED_DN*	The DN of the role that defines the role assignment attributes.	Character (2000)
ROLE_ASSIGNED_DN*	The DN of the role of which the person is a member.	Character (2000)

* Indicates the column is required and not NULL.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

PERSON_ROLE_ASSIGNMENT_VALUES table

The PERSON_ROLE_ASSIGNMENT_VALUES[3] table stores the assignment attribute values. The assignment attributes that a person can have depends on the role membership of a person.

Table 49. The PERSON_ROLE_ASSIGNMENT table

Column name	Description	Data type
RA_ID*	The unique ID of the person role assignment.	Numeric
ATTRIBUTE_NAME*	The role assignment attribute name.	Character (256)
ATTRIBUTE_VALUE*	The role assignment attribute value.	Character (2000)

* Indicates the column is required and not NULL.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

ROLE_ASSIGNMENT_ATTRIBUTES table

The ROLE_ASSIGNMENT_ATTRIBUTES table stores information about assignment attributes that are defined on a static role. A role can have multiple assignment attributes. You can populate this table by running a full or incremental data synchronization in IBM Security Identity Manager.

Table 50. The ROLE_ASSIGNMENT_ATTRIBUTES table

Column name	Description	Data type
ROLE_DN*	Identifies the organizational role to which the attribute belongs.	Character (2000)
ATTRIBUTE_NAME*	Specifies the name of the assignment attribute.	Character (256)
ROLE_NAME	Specifies the name of the role.	Character (256)

* Indicates a required column.

Provisioning policy tables

The tables described in this section are for provisioning policy information.

POLICY_ANALYSIS

The POLICY_ANALYSIS table stores the policy analysis session formation during the policy change and service enforcement change events.

Table 51. POLICY_ANALYSIS table

Column Name	Description	Data type
ANALYSIS_ID*	Unique ID. Primary key.	Character (32)
TENANT_NAME	Name of the tenant in a multi-tenant setting.	Character (64)
STATUS*	Contains status: NOT_STARTED=0 STARTING=1 INITIALIZING=2 PENDING=3 INTERRUPTED=4 ABORTED=5 ERROR=6 COMPLETE=7 INCOMPLETE=8	Numeric
REASON*	Reason for the analysis: POLICY_CHANGE=0 ENFORCEMENT_TYPE_CHANGE=1	Numeric
CONTEXT*	Context of the analysis: SIMULATION=0 ENFORCEMENT=1	Numeric

Table 51. POLICY_ANALYSIS table (continued)

Column Name	Description	Data type
CHANGE_TYPE*	Specific change type: POL_ADD=0 POL_REMOVE=1 POL_MODIFY=2 ENFORCEMENT_CHANGE_ALERT=3 ENFORCEMENT_CHANGE_ENFORCE=4 ENFORCEMENT_CHANGE_SUSPEND=5	Numeric
LAST_ACCESSED*	Last accessed date.	Date
WORKERS_STARTED*	Counter that is incremented when an analysis messaging thread is started and assigned a unit of analysis work. Default: 0	Numeric
WORKERS_COMPLETED*	This counter is incremented when an analysis messaging thread completes its work. Default: 0	Numeric
WORKERS_TOTAL*	The number of messaging threads that do the analysis work. Default: 0	Numeric
ACCOUNT_EVALUATED*	The number of accounts that were evaluated during policy analysis. Default: 0	Numeric

* Indicates the column is required and not null.

POLICY_ANALYSIS_ERROR

The POLICY_ANALYSIS_ERROR table stores non-fatal errors encountered during policy analysis.

Table 52. POLICY_ANALYSIS_ERROR table

Column Name	Description	Data type
ERROR_ID*	Unique identifier of policy analysis error. Primary key.	Character (32)
ENTITY_NAME	Name of an entity.	Character (100)
ENTITY_IDENTIFIER	Global ID.	Character (255)
ENTITY_TYPE	Type of entity: Person=1 Service=2 Account=3 Role=4	Numeric
SERVICE_NAME	Name of the service.	Character (200)
SERVICE_IDENTIFIER	Global ID of the service.	Character (255)
PERSON_NAME	Name of the person.	Character (200)
PERSON_IDENTIFIER	Global ID of the person.	Character (255)
POLICY_NAME	Name of the policy.	Character (100)
POLICY_IDENTIFIER	Global ID of the policy.	Character (255)

Table 52. POLICY_ANALYSIS_ERROR table (continued)

Column Name	Description	Data type
ATTR_NAME	Name of the attribute.	Character (100)
ERROR_TYPE*	Account entity not found Person entity not found Service entity not found Person referential integrity error Role referential integrity error Some generic message	Numeric
ENTITY_ERROR_TYPE	Type of entity error. Values include: 0 – entity not found error 1 – data integrity error	Numeric
ERROR_MESSAGE*	The error message.	Long character
POLICY_ANALYSIS_ID*	Randomly generated session ID. References POLICY_ANALYSIS(ANALYSIS_ID).	Character (32)

* Indicates the column is required and not null.

ACCT_CHANGE

The ACCT_CHANGE table represents general information about account actions that result from a change in a system.

Table 53. ACCT_CHANGE table

Column Name	Description	Data type
CHANGE_ID*	Randomly generated unique ID. Primary key.	Character (32)
ACCT_UID*	The UID of the account.	Character (60)
ACCT_IDENTIFIER*	The UID of the account.	Character (255)
SERVICE_NAME*	Name of the service instance for the account action.	Character (200)
SERVICE_IDENTIFIER*	Global ID.	Character (255)
OWNER_NAME*	Name of the account owner.	Character (200)
OWNER_IDENTIFIER*	Global ID.	Character (255)

Table 53. ACCT_CHANGE table (continued)

Column Name	Description	Data type
OPERATION_TYPE*	Type of operation: DEPROV=0 PROV=1 FLAG_DISALLOWED=2 UNFLAG=3 SUSPEND_DISALLOWED=4 MODIFY=5 ALERT_DISALLOWED=6 FLAG_NONCOMPLIANT=7 SUSPEND_NONCOMPLIANT=8 ALERT_NONCOMPLIANT=9 ERROR=10	Numeric
PROVISION_PRIORITY	Priority of provisioning when there is an ordered sequence with service prerequisites.	Numeric
SEQUENCE_NR	A sequence number.	
REASON*	Enforcement violation reason. Values include: 0 – Disallowed 1 – Not Compliant 2 – Unknown Compliance State	Numeric
REVOKE_CHANGE*	The compound key with a unique analysis session ID and a sequential number of the account action in the analysis.	Numeric
STATUS	The account status. Values include: 0 – Pending 1 - Done	Numeric
POLICY_ANALYSIS_ID*	The analysis session ID this account enforcement action is associated. References POLICY_ANALYSIS(ANALYSIS_ID). Primary key.	Character (32)

* Indicates the column is required and not null.

ATTR_CHANGE

This table represents a single attribute value change.

Table 54. ATTR_CHANGE table

Column Name	Description	Data type
CHANGE_ID*	Sequential identifier for a single attribute change for an account provision or modify action. Primary key.	Character (32)
ATTR_NAME*	Name of the attribute associated with a value operation.	Character (100)

Table 54. ATTR_CHANGE table (continued)

Column Name	Description	Data type
ATTR_VALUE	Value of the attribute associated with the operation.	Character (2000)
OPERATION_TYPE*	Type of attribute operation: ADD=0 REMOVE=1 REPLACE=2	Numeric
PRIVILEGE_ACTION_TYPE*	Type of privilege action associated with the attribute value operation: REVOKATION=0 GRANT=1	Numeric
ATTR_VALUE_PRESENCE*	The old state value of the attribute value before an ADD, REMOVE, or REPLACE operation: ADD=0 REMOVE=1 UNCHANGED=2 UNCHANGED is valid for multi-valued only.	Numeric
POLICY_ANALYSIS_ID*	The analysis session ID. References ACCT_CHANGE(CHANGE_ID).	Character (32)
ACCT_CHANGE_ID*	Account enforcement action ID for the attribute change operation. References ACCT_CHANGE(CHANGE_ID).	Character (32)

* Indicates the column is required and not null.

COMPLIANCE_ALERT table

The COMPLIANCE_ALERT table relates compliance issues to the corresponding compliance alert work item.

Table 55. COMPLIANCE_ALERT table

Column Name	Description	Data type
CA_PROC_ID	Identifier for grouping of related compliance alerts.	Numeric
CA_ISSUE_DN*	Distinguished name of the compliance issue found in the directory server. Primary key.	Character (512)
ACTIVITY_ID	Work item activity ID associated with this compliance issue.	Numeric
ACCOUNT_DN*	Distinguished name of the account associated with this compliance issue.	Character (512)
PARTICIPANT_DN	Participant distinguished name associated with this compliance issue.	Character (512)
STARTED	Status of the compliance issue: 0 – Not Started 1 – Started	Character (1)

* Indicates the column is required and not null.

Recertification policy tables

The tables described in this section are for recertification policy information.

RECERTIFICATIONLOG table

The RECERTIFICATIONLOG[1] table stores recertification policy audit information for account and access recertification policies. This table is used by the Recertification History report. Each row in the table represents the recertification of a single account or access.

Table 56. RECERTIFICATIONLOG table

Column Name	Description	Data type
PROCESS_ID*	The workflow process ID associated with this recertification. Primary key with ACTIVITY_ID.	Numeric
ACTIVITY_ID*	The workflow approval activity ID associated with this recertification. Primary key with PROCESS_ID.	Numeric
ENTITY_DN	The DN of the entity is being recertified (DN of account).	Character (255)
ACCESS_DN	The DN of the access group definition (if access recertification).	Character (255)
ACCOUNT_ID	The user ID of the account that is being recertified.	Character (100)
ACCOUNT_OWNER_NAME	Full name of the owner of the account or access that is being recertified.	Character (100)
ACCOUNT_OWNER	DN of the owner of the account or access that is being recertified.	Character (255)
ACCESS_NAME	The access name of the access that is being recertified.	Character (100)
ACCESS_TYPE	The access type of the access that is being recertified, for example, shared folder or application.	Character (100)
TYPE*	Access or Account recertification. Valid values for this column are: Account (AT) Access (AS)	Character (2)
SERVICE	DN of the service instance to which the account or access that is being recertified belongs.	Character (255)
SERVICE_NAME	The name of the service instance to which the account or access that is being recertified belongs.	Character (100)
SERVICE_PROFILE	The name of the service type to which the service instance belongs.	Character (100)
PARTICIPANT	DN of the person who did the recertification.	Character (255)
PARTICIPANT_NAME	The full name of the person who did the recertification.	Character (100)
PARTICIPANT_ID	The Service user ID of the person who did the recertification.	Character (100)

Table 56. RECERTIFICATIONLOG table (continued)

Column Name	Description	Data type
RECERT_RESULT	The action taken on the approval node in the recertification task. Valid values for this column are as follows: Approved (AA) Rejected (RR) Abort (AO) Timeout – no response (TO) Pending – no response yet, but the request has more time (PE)	Character (2)
ACTION	The action taken on the account/access due to the preceding RECERT_RESULT attribute. Valid values for this column are: Certified (CY) Rejected – Marked (MK) Rejected – Suspended (SD) Rejected – Deleted (DE) Administrator override – certified (AR)	Character (2)
COMMENTS	Text provided by participant of recertification. It might be comments on approval or justification text of override.	Character (2000)
STARTED	Timestamp when recertification started for this account or access.	Character (50)
COMPLETED	Timestamp when recertification completed for this account or access.	Character (50)
RECERT_SUMMARY	Process result summary for this recertification. It is the result summary of the recertification process in general. Valid values are: Success (SS) Warning (SW) Failed (SF)	Character (2)
TENANT	DN of the tenant	Character (255)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.0.

USERRECERT_HISTORY table

The USERRECERT_HISTORY[1] table stores recertification policy audit information for user recertification policies. This table is used by the User Recertification History Report. Each row in the table represents the completion of a user recertification policy approval. Specific resources and decisions that were included in the approval are recorded and described in the following additional tables.

Table 57. USERRECERT_HISTORY table

Column Name	Description	Data type
ID*	A unique identifier for the user recertification approval. Primary key.	Numeric
PROCESS_ID*	The workflow process ID associated with this recertification.	Numeric
ACTIVITY_ID*	The workflow approval activity ID associated with this recertification.	Numeric
PERSON_DN	The DN of the user who is being recertified.	Character (255)
PERSON_NAME	The name of the person who is being recertified.	Character (240)
PERSON_PROFILE	The name of the profile for the person who is being recertified.	Character (128)
PERSON_EMAIL	The email address of the person who is being recertified.	Character (240)
PERSON_CUSTOM_DISPLAY	The custom display attribute of the person who is being recertified.	Character (240)
PERSON_STATUS	The status of the person who is being recertified. The following values are valid: Active (0) Inactive (1)	Numeric
PERSON_CONTAINER_DN	The DN of the container that holds the person who is being recertified.	Character (255)
PERSON_CONTAINER_NAME	The name of the container that holds the person who is being recertified.	Character (128)
POLICY_DN	The DN of the recertification policy that is being run.	Character (255)
POLICY_NAME	The name of the recertification policy that is being run.	Character (240)
SUBMITTED_DATE	Timestamp when recertification started for this account/access.	Character (50)
TIMEOUT	An integer flag that indicates whether the workflow timed out or completed normally. The following values are valid: Completed without timeout (0) Timeout (1)	Numeric

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.1.

USERRECERT_ROLE table

The USERRECERT_ROLE[1] table stores role membership recertification audit information for user recertification policies. This table is used by the User Recertification History Report. Each row in the table represents the approval or rejection of a membership for a user in a particular role. This table references the USERRECERT_HISTORY table through a foreign key.

Table 58. USERRECERT_ROLE table

Column Name	Description	Data type
ID*	A unique identifier for the role entry in this user recertification approval. Primary key.	Numeric

Table 58. USERRECERT_ROLE table (continued)

Column Name	Description	Data type
RECERT_ID*	The unique identifier of this user recertification approval. This field is a foreign key reference to the USERRECERT_HISTORY table ID column.	Numeric
ROLE_DN	The DN of the role that is being recertified.	Character (255)
ROLE_NAME	The name of the role that is being recertified.	Character (240)
ROLE_DESCRIPTION	The description of the role that is being recertified.	Character (500)
DECISION	The decision submitted for this role. The following values are valid: • Approved ("AA") • Rejected ("AR")	Character (2)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.1.

USERRECERT_ACCOUNT table

The USERRECERT_ACCOUNT[1] table stores account recertification audit information for user recertification policies. This table is used by the User Recertification History Report. Each row in the table represents the approval or rejection of an account owned by the user during recertification. This table references the USERRECERT_HISTORY table through a foreign key.

Table 59. USERRECERT_ACCOUNT table

Column Name	Description	Data type
ID*	A unique identifier for the account entry in this user recertification approval. Primary key.	Numeric
RECERT_ID*	The unique identifier of this user recertification approval. This field is a foreign key reference to the USERRECERT_HISTORY table ID column.	Numeric
ACCOUNT_DN*	The DN of the account that is being recertified.	Character (255)
ACCOUNT_UID*	The user ID of the account that is being recertified.	Character (240)
SERVICE_DN*	The DN of the service for the account that is being recertified.	Character (255)
SERVICE_NAME	The name of the service for the account that is being recertified.	Character (240)
SERVICE_DESCRIPTION	The description of the service for the account that is being recertified.	Character (240)
DECISION	The decision submitted for this account. The following values are valid: Approved ("AA") Rejected ("AR") No Decision Required (null)	Character (2)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.1.

USERRECERT_GROUP table

The USERRECERT_GROUP[1] table stores account recertification audit information for user recertification policies. This table is used by the User Recertification History Report. Each row in the table represents the approval or rejection of a group on a user account during user recertification. This table references the USERRECERT_HISTORY and USERRECERT_ACCOUNT tables through foreign keys.

Table 60. USERRECERT_GROUP table

Header	Header	Header
ID*	A unique identifier for the group entry in this user recertification approval. Primary key.	Numeric
RECERT_ID*	The unique identifier of this user recertification approval. This field is a foreign key reference to the USERRECERT_HISTORY table ID column.	Numeric
ACCOUNT_ID*	The unique identifier of the account entry in the recertification approval. This field is a foreign key reference to the USERECERT_ACCOUNT table ID column.	Numeric
GROUP_DN*	The DN of the group that is being recertified.	Character (500)
GROUP_NAME	The name of the group that is being recertified.	Character (240)
GROUP_DESCRIPTION	The description of the group that is being recertified.	Character (500)
DECISION	The decision submitted for this group. The following values are valid: • Approved (“AA”) • Rejected (“AR”)	Character (2)

* Indicates the column is required and not null.

[1] Indicates the column or the value is added in release 5.1.

Shared access tables

IBM Security Identity Manager creates and uses these database tables to store information related to Shared Access Module.

ERCREDENTIALLEASE table

The ERCREDENTIALLEASE[3] table stores the lease information for a checked out credential. If a credential is checked out as a pool member, the table also stores the pool information.

Table 61. ERCREDENTIALLEASE table

Column Name	Description	Data type
DN* ^	The credential lease DN. Primary key.	Character (2000)
ERCVCATALOG* ^	The credential DN.	Character (2000)
ERLESSEE*	The person DN who checked out the credential.	Character (2000)
ERLESSEENAME	The name of the person who checked out the credential.	Character (256)
ERLEASEEXPIRATIONTIME	The lease expiration time.	DATETIME

Table 61. ERCREDENTIALLEASE table (continued)

Column Name	Description	Data type
ERJUSTIFICATION	The business justification for checkout.	Character (2000)
ERLEASESTATUS	Indicates the lease status. Values include: • 0 – active • 1 – inactive indicating the lease is in the process of being checked in or checked out at this moment.	Numeric
ERCREDENTIALPOOLDN	The credential pool DN if the credential is not checked out as a pool member. Otherwise, the value is empty.	Character (2000)
ERCUSTOMATTRIBUTE1 ~ ERCUSTOMATTRIBUTE5	Custom attributes. You can use these 5 custom attributes if you want to extend the lease object to have more information.	Character (2000)
ERLASTNOTIFICATION	The last lease expiration notification time.	DATETIME
ERLEASECREATETIME	The lease creation time.	DATETIME

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

DB_REPLICATION_CONFIG table

The DB_REPLICATION_CONFIG[3] table stores mapping information of the LDAP object replicated to the database table.

Table 62. DB_REPLICATION_CONFIG table

Column Name	Description	Data type
ID	The unique identifier.	Numeric
OBJECT_CLASS_NAME	The LDAP object class name. For example, ercredential.	Character (256)
ATTRIBUTE_NAME	The LDAP attribute name.	Character (256)
DB_TABLE_NAME	The name of the database table which is mapped to the object class in the OBJECT_CLASS_NAME column.	Numeric
KEY_COLUMN_NAME	The primary key column name of the table in the DB_TABLE_NAME column.	Character (256)
REPLICATE_COLUMN_NAME	The name of the column, which is mapped to the attribute name in the ATTRIBUTE_NAME column.	Character (256)
MULTI_VALUE	Indicates whether the attribute is multivalue attribute. Values include: • y – multivalue attribute • n – single-value attribute	Character (1)

Table 62. DB_REPLICATION_CONFIG table (continued)

Column Name	Description	Data type
UPDATE_ONLY	Indicates whether the attribute replication is only for object update. Values include: • y – for update only • n – for add, update, and delete	Character (1)
CASE_SENSITIVE	Indicates whether the attribute value is not case-sensitive: • y – case sensitive • n – not case-sensitive	Character (1)

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_BULK_LOAD table

The SA_BULK_LOAD[3] table stores the shared access batch load request data.

Table 63. SA_BULK_LOAD table

Column Name	Description	Data type
LOAD_ID*	The unique identifier for the shared access batch load request. Primary key.	Character (255)
DATA_CLOB	The shared access batch load data.	Big Data

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_CREDPOOL_DESCRIPTION table

The SA_CREDPOOL_DESCRIPTION[3] table stores the description of a credential pool. Each credential pool might have zero or multiple descriptions.

Table 64. SA_CREDPOOL_DESCRIPTION table

Column Name	Description	Data type
DN*	The credential pool DN.	Character (2000)
DESCRIPTION	The description of credential pool.	Character (2000)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_CREDPOOL_GROUP table

The SA_CREDPOOL_GROUP[3] table stores the group definition of a credential pool. Each credential pool might consist of one or multiple groups.

Table 65. SA_CREDPOOL_GROUP table

Column Name	Description	Data type
DN*	The credential pool DN.	Character (2000)
ERSERVICEGROUP	The DN of the service group.	Character (2000)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_CREDPOOL_OWNER table

The SA_CREDPOOL_OWNER[3] table stores the owner of a credential pool. Each credential pool might have zero or multiple owners. A pool owner can be an organizational role or a person.

Table 66. SA_CREDPOOL_OWNER table

Column Name	Description	Data type
DN*	The credential pool DN.	Character (2000)
OWNER	The DN of the POOL owner. The owner can be an organizational role or a person.	Character (2000)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_EVALUATION_BU table

The SA_EVALUATION_BU[3] table stores organizational container information.

Table 67. SA_EVALUATION_BU table

Column Name	Description	Data type
DN* ^	The DN of the organizational container. Primary key.	Character (2000)
NAME	The name of the organizational container.	Character (256)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_EVALUATION_BU_HIERARCHY table

The SA_EVALUATION_BU_HIERARCHY[3] table stores the flattened organizational container hierarchy tree.

Table 68. SA_EVALUATION_BU_HIERARCHY table

Column Name	Description	Data type
BU_DN* ^	The DN of the organizational container. Primary key.	Character (2000)
CHILD_DN*	The DN of the child container.	Character (2000)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_EVALUATION_CREDENTIAL table

The SA_EVALUATION_CREDENTIAL[3] table stores credential information relevant to shared access authorization evaluation.

Table 69. SA_EVALUATION_CREDENTIAL table

Column Name	Description	Data type
DN*^	The credential DN. Primary key.	Character (2000)
ACCOUNT_DN	The account DN.	Character (2000)
ACCOUNT_UID	The account user ID.	Character (256)
USE_GLOBAL_SETTINGS	Indicates whether use global setting for the credential. Value includes: • 0 – use global setting • 1 – use the own setting of the credential	Numeric
IS_SEARCHABLE	Indicates whether the credential is available for checkout search. Values includes: • 0 – search enabled • 1 – search disabled, credential is intended to be checked out only as pool member	Numeric
IS_EXCLUSIVE	Indicates the credential access mode. Values include: • 0 – exclusive • 1 – non-exclusive • 2 – non-shared	Numeric
IS_PASSWORD_VIEWABLE	Indicates whether the password can be displayed to user. Values include: • 0 – viewable • 1 – not viewable	Numeric
ACCOUNT_STATUS	Indicates the account status. Values include: • 0 – active • 1 – inactive	Numeric
SERVICE_DN^	The global identifier of the credential service. **Note:** For legacy credentials created in IBM Security Privileged Identity Manager 1.0, this column stores the service DN string.	Character (2000)
RESET_PASSWORD	Indicates whether the password is reset during checkin. Values include: • 0 – password is reset • 1 – password not changed	Numeric

Table 69. SA_EVALUATION_CREDENTIAL table (continued)

Column Name	Description	Data type
MAX_CHECKOUT_TIME	The maximum checkout duration in hours.	Numeric
OBJECTPROFILE_NAME#	This attribute is not used.	Character (255)
NAME	Credential name.	Character (255)
OWNERSHIP_TYPE	The account ownership type.	Character (255)
OWNER_DN	The account owner DN.	Character (2000)
BU_DN^	The DN of the organizational container where the credential is created. **Note:** For legacy credentials created in IBM Security Privileged Identity Manager 1.0, this column is NULL.	Character (2000)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

# Indicates the column is currently not being used. The value is always NULL.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_EVAL_CRED_DESCRIPTION table

The SA_EVAL_CRED_DESCRIPTION[3] table stores the description of a credential. Each credential might have zero or multiple descriptions.

Table 70. SA_EVAL_CRED_DESCRIPTION table

Column Name	Description	Data type
DN*^	The credential DN.	Character (2000)
DESCRIPTION	The description of credential.	Character (2000)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_EVALUATION_CREDENTIAL_POOL table

The SA_ EVALUATION_CREDENTIAL_POOL[3] table stores credential pool information relevant to shared access authorization evaluation.

Table 71. SA_ EVALUATION_CREDENTIAL_POOL table

Column Name	Description	Data type
DN*	The credential DN. Primary key.	Character (2000)
NAME	The pool name.	Character (256)

Table 71. SA_ EVALUATION_CREDENTIAL_POOL table (continued)

Column Name	Description	Data type
SERVICE_DN^	The service DN.	Character (2000)
BU_DN^	The DN of the organizational container where the pool is created.	Character (2000)
USE_GLOBAL_SETTINGS#	This column is not used.	Numeric
OBJECTPROFILE_NAME#	This column is not used.	Character (255)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

# Indicates the column is currently not being used. The value is always NULL.

3 Indicates the table is added in IBM Security Identity Manager 6.0.

SA_EVALUATION_SERVICE table

The SA_EVALUATION_SERVICE[3] table stores service, which contains either credentials in the vault or credential pools. This table stores only the service information relevant to shared access authorization evaluation.

Table 72. SA_EVALUATION_SERVICE table

Column Name	Description	Data type
DN* ^	The service DN. Primary key.	Character (2000)
NAME	The service name.	Character (256)
TYPE	The service profile name.	Character (256)
BU_DN^	The DN of the organizational container.	Character (2000)
ID[4]	The unique identifier of the service.	Long Integer
ENFORCEMENT[4]	The service enforcement action.	Short Integer

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

3 Indicates the table is added in IBM Security Identity Manager 6.0.

4 Indicates that the column is added in IBM Security Identity Manager 6.0.0.2.

SA_EVALUATION_SERVICE_TAG table

The SA_EVALUATION_SERVICE_TAG[3] table stores the service tag information for services stored in SA_EVALUATION_SERVICE or SA_VAULT_SERVICE. Each service might have zero or multiple tags.

Table 73. SA_EVALUATION_SERVICE_TAG table

Column Name	Description	Data type
SERVICE_DN* ^	• Stores the service DN if the tag is defined for the service from the SA_EVALUATION_SERVICE table. • Stores the service id if the tag is defined for the credential service from the SA_VAULT_SERVICE table.	Character (2000)
TAG	The service tag.	Character (500)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_GLOBAL_CONFIGURATION table

The SA_GLOBAL_CONFIGURATION[3] table stores information about the shared access global configuration settings. This table has only one row.

Table 74. The SA_GLOBAL_CONFIGURATION table

Column name	Description
ACCESS_MODE	Specifies the access mode of credentials. • 0: Indicates exclusive permissions. • 1: Indicates non-exclusive permissions. • 2: Indicates non-shared credentials.
MAX_CHECKOUT_DURATION	Specifies the duration for which a credential can be checked out. You must specify this attribute if the access is exclusive. Specify the time in weeks, days, or hours by adding the suffix, as described in the following examples: • 8 w: Indicates 8 weeks. • 8 d: Indicates 8 days. • 8 h: Indicates 8 hours. By default, the duration is considered in hours if no suffix is specified. The default duration is 8 h.
PASSWORD_VIEWABLE	Specifies whether to show the credential password to users on the IBM Security Identity Manager Self-service user interface or the Identity Service Center user interface. You must specify this attribute if the access mode value is 0 (TRUE) or 1 (FALSE). The default value is FALSE, which indicates that the credential password must not be shown.

Table 74. The SA_GLOBAL_CONFIGURATION table (continued)

Column name	Description
SHAREDACCOUNT_SEARCH	Specifies whether checkout search must be enabled for the credential on the Self-service user interface or the Identity Service Center user interface. The valid values are: • 0 for enabling the checkout search. • 1 for disabling the checkout search.
PASSWORD_RESET	Specifies whether account password to reset when the corresponding checked out credential is checked in. The valid values are: • 0: Indicates that the password must be reset. • 1: Indicates that password must not be reset.
OPERATION_NAME	Specifies the global lifecycle operation that starts the checkout workflow extension.
LEASE_EXP_HANDLING	Specifies the value T in the database that indicates that the lease expiration monitoring is enabled. **Note:** This column is for internal use only.
LEASE_EXP_HANDLING_OPTION	Specifies the following information: • 0 if the **Notify Violation** option is selected. • 1 if the **Notify Violation and check in** option is selected.
VIOLATION_NOTIFY_PARTICIPANT	Specifies the recipient who is authorized to receive the lease expiration notifications. The name is stored as specific string in the database that depends on the recipient, for example, SA for Administrator.
NOTIFICATION_PARTICIPANT_DN	Specifies the Distinguished Name (DN) of the recipients whom you want to notify. The maximum DN character limit is 256 in the database.
SCHEDULE_FREQUENCY_MINUTE	Specifies the duration after which you want IBM Security Identity Manager to check for the expired leases. The time is stored in minutes and the default is 60 minutes.
NOTIFY_FREQUESNCY_MINUTE	Specifies the time interval to send notification to the recipients to remind them about lease expiration. The time is in minutes and the default is 1440 minutes.

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_POLICY table

The SA_POLICY[3] table stores shared access policy information.

Table 75. SA_POLICY table

Column Name	Description	Data type
ID*	Unique identifier. Primary key.	NUMERIC
DN	Distinguished Name of the policy.	Character (2000)
BU_DN^	Distinguished Name of the organization container.	Character (2000)

Table 75. SA_POLICY table (continued)

Column Name	Description	Data type
SCOPE	The policy scope. Values include: • 1 – one level • 2 – sub tree	NUMERIC
STATUS	The policy status. Values include: • 0 – active • 1 – inactive	NUMERIC
POLICY_NAME	The policy name.	Character (255)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_POLICY_DESCRIPTION table

The SA_POLICY_DESCRIPTION[3] table stores the description of a shared access policy. Each policy might have zero or multiple descriptions.

Table 76. SA_POLICY_DESCRIPTION table

Column Name	Description	Data type
POLICY_ID*	ID of the policy ID associated with the description.	Numeric
DESCRIPTION	Distinguished Name of the organizational role, or * indicates all people.	Character (2000)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_POLICY_ENTITLEMENT table

The SA_POLICY_ENTITLEMENT[3] table stores the shared access policy entitlements. Each policy might have one or multiple entitlements.

Table 77. SA_POLICY_ENTITLEMENT table

Column Name	Description	Data type
ID*	Unique global ID. Primary key.	Numeric
POLICY_ID*	ID of the policy ID associated with the entitlement.	Numeric
TYPE	The entitlement type. Values include: • 0 – Credential • 1 – Credential pool	Numeric

Table 77. SA_POLICY_ENTITLEMENT table (continued)

Column Name	Description	Data type
DEFINITION_TYPE	The entitlement definition type. Values include: • 0 – specific credential object entitlement • 1 – filter entitlement	Numeric
NAME	The entitlement name.	Character (256)
TARGET_NAME	The account uid or pool name that matches the string.	Character (256)
SERVICE_TYPE	The service profile name.	Character (256)
SERVICE_NAME	The service name that matches the string.	Character (256)
SERVICE_GROUP	The service tag that matches the string.	Character (500)
TARGET_DN^	The credential or pool DN.	Character (2000)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_POLICY_ERURI table

The SA_POLICY_ERURI[3] table stores the universal resource identifier of a shared access policy. Each policy might have zero or multiple universal resource identifiers.

Table 78. SA_POLICY_ERURI table

Column Name	Description	Data type
POLICY_ID*	ID of the policy ID associated with the universal resource identifier.	Numeric
ERURI	The universal resource identifier.	Character (2000)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_POLICY_MEMBERSHIP table

The SA_POLICY_MEMBERSHIP[3] table stores the shared access policy memberships. Each policy might have one or multiple memberships.

Table 79. SA_POLICY_MEMBERSHIP table

Column Name	Description	Data type
ID*	Unique ID. Primary key.	Numeric
POLICY_ID*	ID of the policy ID associated with the membership.	Numeric

Table 79. SA_POLICY_MEMBERSHIP table (continued)

Column Name	Description	Data type
ROLE_DN	Distinguished Name of the organizational role. The value can be a role DN or *, which indicates all people.	Character (2000)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

SA_VAULT_SERVICE table

The SA_VAULT_SERVICE[4] table stores credential service information.

Table 80. SA_VAULT_SERVICE table

Column Name	Description	Data type
ID*^	The global identifier of the credential service. Primary key.	Character (2000)
SERVICE_URI*^	The unique resource identifier of the credential service.	Character (500)
TYPE	The type of the credential service.	Character (256)
NAME	The name of the credential service.	Character (256)
BU_DN^	The DN of the organizational container.	Character (2000)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[4] Indicates the table is added in IBM Security Identity Manager 6.0.0.2.

SA_VAULT_SERVICE_ALIAS table

The SA_VAULT_SERVICE_ALIAS[4] table stores the credential service aliases. Each credential service might have zero or multiple aliases.

Table 81. SA_VAULT_SERVICE_ALIAS table

Column Name	Description	Data type
SERVICE_ID*^	The global identifier of the credential service.	Character (20)
SERVICE_ALIAS*	The service tag.	Character (500)

* Indicates the column is required and not null.

^ Indicates the column is associated with a generated lowercase column with name L_*columnName*.

[4] Indicates the table is added in IBM Security Identity Manager 6.0.0.2.

SYNCH_OBJECT_LOCK table

The SYNCH_OBJECT_LOCK[3] table is used for locking objects during update to prevent data replication target object out of synch with the replication source.

Table 82. SYNCH_OBJECT_LOCK table

Column Name	Description	Data type
OBJ_ID*	The DN of the object. Primary key.	Character (2000)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

V_AUTHORIZED_CREDENTIALS view

The V_AUTHORIZED_CREDENTIALS[3] view returns the authorized credentials by policy, role, and entitlement.

Table 83. V_AUTHORIZED_CREDENTIALS view

Column Name	Description	Data type
CRED_DN	The credential DN.	Character (2000)
CRED_ACCOUNT_DN	The account DN.	Character (2000)
CRED_ACCOUNT_UID	The account user ID.	Character (256)
EXCLUSICE_ACCESS	Indicates the credential access mode. Values include: • 0 – exclusive • 1 – non-exclusive • 2 – non-shared	Numeric
SA_MEMBER_ROLE_DN	Distinguished Name of the Organizational role. The value can be a role DN or *, which indicates all people.	Character (2000)
SERVICE_DN	The service DN.	Character (2000)
SERVICE	The service name.	Character (256)
SERVICE_BUDN	The DN of the organizational container where the service is located.	Character (2000)
SERVICE_BU	The name of the organizational container where the service is located.	Character (256)
SA_POLICY_ID	The policy unique identifier.	Numeric
POLICY_NAME	The policy name.	Character (255)
SA_ENTITLEMENT_ID	The entitlement unique identifier.	Numeric

[3] Indicates the view is added in IBM Security Identity Manager 6.0.

V_AUTHORIZED_CREDENTIALPOOLS view

The V_AUTHORIZED_CREDENTIALPOOLS[3] view returns the authorized credential pools by policy, role, and entitlement.

Table 84. V_AUTHORIZED_CREDENTIALPOOLS view

Column Name	Description	Data type
CREDPOOL_DN	The credential DN.	Character (2000)

Table 84. V_AUTHORIZED_CREDENTIALPOOLS view (continued)

Column Name	Description	Data type
CREDPOOL_NAME	The pool name.	Character (256)
GROUP_DN	The account user ID.	Character (2000)
SA_MEMBER_ROLE_DN	Distinguished Name of the organizational role. The value can be a role DN or *, which indicates all people.	Character (2000)
SERVICE_DN	The service DN.	Character (2000)
SERVICE	The service name.	Character (256)
SERVICE_BUDN	The DN of the organizational container where the service is located.	Character (2000)
SERVICE_BU	The name of the organizational container where the service is located.	Character (256)
SA_POLICY_ID	The policy unique identifier.	Numeric
POLICY_NAME	The policy name.	Character (255)
SA_ENTITLEMENT_ID	The entitlement unique identifier.	Numeric

[3] Indicates the view is added in IBM Security Identity Manager 6.0.

V_SA_EVALUATION_SERVICE view

The V_SA_EVALUATION_SERVICE[4] view returns the union of SA_EVALUATION_SERVICE and SA_VAULT_SERVICE.

Table 85. V_SA_EVALUATION_SERVICE view

Column Name	Description	Data type
DN	The global identifier of the credential service. **Note:** For legacy credentials created in IBM Security Privileged Identity Manager 1.0, this column stores the service DN string.	Character (2000)
NAME	The service name.	Character (256)
TYPE	The service type.	Character (256)
BU_DN	The DN of the organizational container.	Character (2000)

[4] Indicates the view is added in IBM Security Identity Manager 6.0.0.2.

V_SAPOLICY_ENTITLEMENT_DETAIL view

The V_SAPOLICY_ENTITLEMENT_DETAIL[3] view returns the shared access policy and entitlement details.

Table 86. V_SAPOLICY_ENTITLEMENT_DETAIL view

Column Name	Description	Data type
SAPENTITLE_DN	The DN of the shared access policy.	Character (2000)
SAPENTITLE_TYPE	The entitlement type. Values include: • 0 – Credential • 1 – Credential pool	Numeric

Table 86. V_SAPOLICY_ENTITLEMENT_DETAIL view (continued)

Column Name	Description	Data type
SAPENTITLE_DEFINITION_TYPE	The entitlement definition type. Values include: • 0 – specific credential object entitlement • 1 – filter entitlement	Numeric
SAPENTITLE_NAME	The entitlement name.	Character (256)
SAPENTITLE_TARGET_NAME	The matching string of account uid or pool name.	Character (2000)
SAPENTITLE_SERVICE_TYPE	The service profile name.	Character (256)
SAPENTITLE_SERVICE_NAME	The matching string of the service name.	Character (2000)
SAPENTITLE_SERVICE_GROUP	The matching string of the service tag.	Character (256)
SAPENTITLE_TARGET_DN	The credential or pool DN if the entitlement definition type is 0, otherwise, the value is empty.	Numeric

[3] Indicates the view is added in IBM Security Identity Manager 6.0.

Access catalog tables and views

IBM Security Identity Manager creates and uses these database tables and views to store information related to Access Catalog.

T_AccessCatalog table

The T_AccessCatalog[4] table stores information about the access, including name, description, category, badge, and search terms. The access information is displayed in the **Request Access** user interface in the Identity Service Center.

Table 87. T_AccessCatalog table

Column Name	Description	Data type
entity_id*	The unique identifier of the access.	Big integer
entity_type*	The entity type of the access. Supported access types are: 1: Service 2: Group 3: Role	Small integer
name*^	Access name.	Character (255)
description^	Access description.	Character (2000)

Table 87. T_AccessCatalog table (continued)

Column Name	Description	Data type
view_option	Indicates whether access is enabled in Request Access and whether it is a common requested access: 1: Access Disabled 2: Enabled 3: Enabled as common access **Note:** Common access is used only in **Access Request** in the self-service console and administrative console; it is not supported in the Identity Service Center.	Small integer
Category	Access category.	Character (1000)
icon_url	The URL of the icon of the access. This icon is displayed when the user searches for the access in the Identity Service Center.	Character (255)
additionalinfo^	Additional information about the access. This information is displayed in the access card when the user searches for the access in the Identity Service Center.	Character (2000)

* Indicates that the column is required and not null.

^ Indicates that the column is associated with a generated lowercase column with name L_*columnName*. Use this column if the search is not case sensitive.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_AccessCatalogTags table

The T_AccessCatalogTags[4] table stores the access search terms. Each access can have zero or many search terms defined.

Table 88. T_AccessCatalogTags table

Column Name	Description	Data type
tag ^	Access search term.	Character (100)
access_id*	Access identifier.	Big integer

* Indicates that the column is required and not null.

^ Indicates that the column is associated with a generated lowercase column with name L_*columnName*. Use this column if the search is not case sensitive.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_BADGES table

The T_BADGES[4] table stores the access badge information.

Table 89. T_BADGES table

Column Name	Description	Data type
ENTITY_ID	Access identifier.	Big integer
BADGE_TEXT^	The key of the badge text, which is localized for supported languages.	Character (1000)
BADGE_STYLE	The style used to display the badge. For example, if the style is green, it indicates that badge is displayed in green color.	Character (2000)

^ Indicates that the column is associated with a generated lowercase column with name L_*columnName*. Use this column if the search is not case sensitive.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_Owner table

The T_Owner[4] table stores the access owner information.

Table 90. T_Owner table

Column Name	Description	Data type
type	Owner type: 1: Role 2: Person	Small integer
owner_dn	Distinguished name of the owner.	Character (2000)
access_id*	Access identifier.	Big integer

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_GROUP table

The T_GROUP[4] table stores the information for group entities.

Table 91. T_GROUP table

Column Name	Description	Data type
Type*	Name of the group profile.	Character (256)
Rdn*	RDN attribute of the group.	Character (1000)
dn	Distinguished Name of the group	Character (2000)
service_id*	Service identifier of the group	Big integer
Id*	Unique identifier of the group	Big integer

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_Role table

The T_Role[4] table stores the information for the role entities.

Table 92. T_Role table

Column Name	Description	Data type
Id*	Unique identifier of the role.	Big integer
Dn*	Distinguished name of the role.	Character (2000)
bu_dn*^	Distinguished name of the business unit of the role	Character (2000)

* Indicates that the column is required and not null.

^ Indicates that the column is associated with a generated lowercase column with name L_*columnName*. Use this column if the search is not case sensitive.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_ProvisioningPolicy table

The T_ProvisioningPolicy[4] table stores the information for provisioning policies. This information is replicated from LDAP to the database to optimize performance when searching for authorized access.

Table 93. T_ProvisioningPolicy table

Column Name	Description	Data type
Id*	Unique identifier of the provisioning policy.	Big integer
Dn*	Distinguished name of the provisioning policy.	Character (2000)
Name*	Name of the provisioning policy.	Character (256)
scope	Scope of the provisioning policy. 1: Single-level 2: Sub-tree	Small integer
status	Indicates whether the policy is active or not. 0: Active 1: Inactive	Small integer
Bu*^	Distinguished name of the business unit of the provisioning policy.	Character (2000)
priority	Priority of the policy.	Big integer

* Indicates that the column is required and not null.

^ Indicates that the column is associated with a generated lowercase column with name L_*columnName*.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_PolicyMembership table

The T_PolicyMembership[4] table stores the information for the memberships of a provisioning policy.

Table 94. T_PolicyMembership table

Column Name	Description	Data type
policy_id*	Identifier of the provisioning policy.	Big integer
role_id*	Identifies the role membership. Can be either of the following: The keyword EVERYONE or OTHERS The identifier of the role as a string	Character (100)

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_ServiceEntitlement table

The T_ServiceEntitlement[4] table stores the information for the service entitlement of a provisioning policy.

Table 95. T_ServiceEntitlement table

Column Name	Description	Data type
Id*	System-generated ID of the service entitlement.	Big integer
policy_id*	Identifier of the provisioning policy.	Big integer
target_type	Service target type. 0: Service profile 1: Service instance 2: All services 3: Host selection policy target	Small integer
target_profile	Service profile.	Character (100)
target_id	Identifier of the service. This column is applicable only when the target type is 1 (service instance).	Big integer
Priority*	Service entitlement priority. This is a system-calculated value based on the policy membership type, service entitlement target type, and service entitlement ownership type. Do **not** modify this column manually.	Small integer
ownership_type	Account ownership type to which the service entitlement is applicable.	Character (20)

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_AttributeEntitlement table

The T_AttributeEntitlement[4] table stores the information for the entitled attribute values of a service entitlement in a provisioning policy.

Table 96. T_AttributeEntitlement table

Column Name	Description	Data type
se_id*	Identifier of the service entitlement.	Big integer
attr_name*	Name of the account attribute.	Character (100)
attr_value	Stores an attribute value whose value_type is Regular Expression(20) or Constant value(30).	Character (2000)
Type*	Type of entitlement. 0: Excluded. Implies that all values are granted except for the specified value in the attr_value column. 1: Allowed. Implies that the specific value in the attr_value column is granted 2: Default. Implies that the specified value in the attr_value column is a default. Default values are considered granted as well. 3: Mandatory. Implies that the specified value in the attr_value column is required.	Small integer
value_type	The value type, which defines the format of the value. 10: JavaScript 20: Regular Expression 30: Constant value	Small integer
JS_ATTR_VALUE	Stores an attribute value whose value_type is JavaScript(10).	Long character

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_ServiceTags table

The T_ServiceTags[4] table stores the information for service tags for a service entitlement in a provisioning policy.

Table 97. T_ServiceTags table

Column Name	Description	Data type
se_id*	Identifier of the service entitlement.	Big integer
Tag*	Service tag. For each service entitlement, there can be zero or many tags defined.	Character (100)

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

TMP_HostSEByPerson table

The TMP_HostSEByPerson[4] table stores the information for service targets that are applicable to a specific user according to the host selection policy when a service

entitlement target type is host selection policy. Information in this table is dynamically generated during service or group authorization for a specific user, and it is associated with a unique transaction ID that corresponds to the authorization evaluation process. The data is automatically removed by the system upon completion of the authorization evaluation process.

Table 98. TMP_HostSEByPerson table

Column Name	Description	Data type
se_id*	Identifier of the service entitlement.	Big integer
transaction_id*	System-generated transaction ID for the service or group access evaluation.	Big integer
target_id*	The service identifier of the service target, based on the host selection policy.	Big integer
target_dn*	The distinguished name of the service target, based on the host selection policy.	Character (2000)

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

TMP_JSAEByPerson table

The TMP_JSAEByPerson[4] table stores the information for the evaluated JavaScript attribute values for a specific user according to the attribute entitlements with the JavaScript value type in a provisioning policy. Information in this table is dynamically generated during service or group authorization for a specific user, and it is associated with a unique transaction ID that corresponds to the authorization evaluation process. The data is automatically removed by the system upon completion of the authorization evaluation process.

Table 99. TMP_JSAEByPerson table

Column Name	Description	Data type
se_id*	Identifier of the service entitlement.	Big integer
transaction_id*	System generated transaction ID for the service or group access evaluation.	Big integer
attr_name*	Attribute name.	Character (100)
attr_value*	Evaluated attribute value based on the JavaScript.	Character (2000)
service_id*	Identifier of the service.	Big integer

* Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_Global_Settings table

The T_Global_Settings[4] table stores the global configuration properties for IBM Security Identity Manager that are required for service and group authorization evaluation.

Table 100. T_Global_Settings table

Column Name	Description	Data type
name	Name of the system property.	Character (255)
value	Value of the system property.	Character (255)

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_GROUP_PROFILE table

The T_GROUP_PROFILE[4] table stores the group profile information.

Table 101. T_GROUP_PROFILE table

Column Name	Description	Data type
name*	Profile name.	Character (100)
rdn_attr*	Name of the account attribute for group membership.	Character (100)
acct_attr*	Name of the account attribute for group membership	Character (100)
case_sensitivity	Used for regression expression match for group. 0: Case sensitive 2: Not case sensitive	Integer

[*] Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

T_Joindirective table

The T_Joindirective[4] table stores the attribute join directive definitions.

Table 102. T_Joindirective table

Column Name	Description	Data type
attr_name*	Name of the attribute	Character (100)
joinDirective*	Name of the attribute join directive. 0: Priority Join 3: Union Join	Small integer

[*] Indicates that the column is required and not null.

[4] Indicates that the table is added in IBM Security Identity Manager 6.0.0.2.

V_GroupCatalog view

The V_GroupCatalog[4] view provides information for groups in the access catalog.

Table 103. V_GroupCatalog view

Column Name	Description
ID	See the **entity_id** column in "T_AccessCatalog table" on page 56.

Table 103. V_GroupCatalog view (continued)

Column Name	Description
NAME	See the **name** column in "T_AccessCatalog table" on page 56.
L_NAME	See the **name** column in "T_AccessCatalog table" on page 56.
DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
L_DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
CATEGORY	See the **Category** column in "T_AccessCatalog table" on page 56.
VIEW_OPTION	See the **view_option** column in "T_AccessCatalog table" on page 56.
ICON_URL	See the **icon_url** column in "T_AccessCatalog table" on page 56.
ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.
L_ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.
DN	See the **dn** column in "T_GROUP table" on page 58.
PROFILE	See the **Type** column in "T_GROUP table" on page 58.
BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
L_BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
RDN	See the **Rdn** column in "T_GROUP_PROFILE table" on page 63.
SERVICE_DN	See the **DN** column in "SA_EVALUATION_SERVICE table" on page 48.
SERVICE_ID	See the **ID** column in "SA_EVALUATION_SERVICE table" on page 48.
ACCT_ATTR	See the **acct_attr** column in "T_GROUP_PROFILE table" on page 63.
CASE_SENSITIVITY	See the **case_sensitivity** column in "T_GROUP_PROFILE table" on page 63.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

V_RoleCatalog view

The V_RoleCatalog[4] view provides information for roles in the access catalog.

Table 104. V_RoleCatalog view

Column Name	Description
ID	See the **entity_id** column in "T_AccessCatalog table" on page 56.
NAME	See the **name** column in "T_AccessCatalog table" on page 56.

Table 104. V_RoleCatalog view (continued)

Column Name	Description
L_NAME	See the **name** column in "T_AccessCatalog table" on page 56.
DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
L_DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
CATEGORY	See the **Category** column in "T_AccessCatalog table" on page 56.
VIEW_OPTION	See the **view_option** column in "T_AccessCatalog table" on page 56.
ICON_URL	See the **icon_url** column in "T_AccessCatalog table" on page 56.
DN	See the **Dn** column in "T_Role table" on page 59.
BU_DN	See the **bu_dn** column in "T_Role table" on page 59.
L_BU_DN	See the **bu_dn** column in "T_Role table" on page 59.
ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.
L_ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

V_ServiceCatalog view

The V_ServiceCatalog[4] view provides information for services in the access catalog.

Table 105. V_ServiceCatalog view

Column Name	Description
ID	See the **entity_id** column in "T_AccessCatalog table" on page 56.
NAME	See the **name** column in "T_AccessCatalog table" on page 56.
L_NAME	See the **name** column in "T_AccessCatalog table" on page 56.
DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
L_DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
CATEGORY	See the **Category** column in "T_AccessCatalog table" on page 56.
VIEW_OPTION	See the **view_option** column in "T_AccessCatalog table" on page 56.
ICON_URL	See the **icon_url** column in "T_AccessCatalog table" on page 56.
DN	See the **dn** column in "SA_EVALUATION_SERVICE table" on page 48.

Table 105. V_ServiceCatalog view (continued)

Column Name	Description
PROFILE	See the **Type** column in "SA_EVALUATION_SERVICE table" on page 48.
BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
L_BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.
L_ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

V_DYNAMIC_ENTITLEMENT view

The V_DYNAMIC_ENTITLEMENT[4] view provides information for entitlements in the provisioning policy that need to be dynamically evaluated.

Table 106. V_DYNAMIC_ENTITLEMENT view

Column Name	Description
SE_TYPE	Dynamic entitlement type. 0: Host selection policy entitlement 1: JavaScript attribute entitlement
SE_ID	Identifier of the service entitlement. See the **Id** column in "T_ServiceEntitlement table" on page 60.
TRANSACTION_ID	Transaction ID of the authorization process. Maps to the **transaction_id** column in either "TMP_HostSEByPerson table" on page 61 or "TMP_JSAEByPerson table" on page 62.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

V_ServiceEntitlementByRole view

The V_ServiceEntitlementByRole[4] view provides information about service entitlements by role.

Table 107. V_ServiceEntitlementByRole view

Column Name	Description
ROLE_ID	See the **Id** column in "T_Role table" on page 59.
SERVICE_ID	See the **ID** column in "SA_EVALUATION_SERVICE table" on page 48.
SERVICE_DN	See the **DN** column in "SA_EVALUATION_SERVICE table" on page 48.
L_SERVICE_DN	See the **DN** column in "SA_EVALUATION_SERVICE table" on page 48.
SE_REF_ID	See the **Id** column in "T_ServiceEntitlement table" on page 60.

Table 107. V_ServiceEntitlementByRole view (continued)

Column Name	Description
SE_PRIORITY	See the **Priority** column in "T_ServiceEntitlement table" on page 60.
POLICY_ID	See the **policy_id** column in "T_ServiceEntitlement table" on page 60.
POLICY_DN	See the **Dn** column in "T_ProvisioningPolicy table" on page 59.
POLICY_PRIORITY	See the **priority** column in "T_ProvisioningPolicy table" on page 59.
OWNERSHIP_TYPE	See the **ownership_type** column in "T_ServiceEntitlement table" on page 60.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

V_GROUP_PROFILE view

The V_GROUP_PROFILE[4] view provides metadata for groups.

Table 108. V_GROUP_PROFILE view

Column Name	Description
NAME	Group profile name. See the **name** column in "T_GROUP_PROFILE table" on page 63.
RDN_ATTR	RDN attribute name. See the **rdn_attr** column in "T_GROUP_PROFILE table" on page 63.
ACCT_ATTR	Group membership account attribute name. See the **acct_attr** column in "T_GROUP_PROFILE table" on page 63.
JOINDIRECTIVE	Join directive of the group attribute. See the **joinDirective** column in "T_Joindirective table" on page 63.
CASE_SENSITIVITY	Case sensitivity for regular expression evaluation. See the **case_sensitivity** column in "T_GROUP_PROFILE table" on page 63.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

V_GC_INTERSECT view

The V_GC_INTERSECT[4] view provides information for groups in the access catalog that use intersection join in the provisioning policy.

Table 109. V_GC_INTERSECT view

Column Name	Description
ID	See the **entity_id** column in "T_AccessCatalog table" on page 56.
NAME	See the **name** column in "T_AccessCatalog table" on page 56.
L_NAME	See the **name** column in "T_AccessCatalog table" on page 56.

Table 109. V_GC_INTERSECT view (continued)

Column Name	Description
DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
L_DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
CATEGORY	See the **Category** column in "T_AccessCatalog table" on page 56.
VIEW_OPTION	See the **view_option** column in "T_AccessCatalog table" on page 56.
ICON_URL	See the **icon_url** column in "T_AccessCatalog table" on page 56.
DN	See the **dn** column in "T_GROUP table" on page 58.
PROFILE	See the **Type** column in "T_GROUP table" on page 58.
BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
L_BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
RDN	See the **rdn_attr** column in "T_GROUP_PROFILE table" on page 63.
SERVICE_DN	See the **DN** column in "SA_EVALUATION_SERVICE table" on page 48.
SERVICE_ID	See the **ID** column in "SA_EVALUATION_SERVICE table" on page 48.
ACCT_ATTR	See the **acct_attr** column in "T_GROUP_PROFILE table" on page 63.
CASE_SENSITIVITY	See the **case_sensitivity** column in "T_GROUP_PROFILE table" on page 63.
TAG	See the **tag** column in "T_AccessCatalogTags table" on page 57.
L_TAG	See the **tag** column in "T_AccessCatalogTags table" on page 57.
BADGE_TEXT	See the **BADGE_TEXT** column in "T_BADGES table" on page 58.
BADGE_STYLE	See the **BADGE_STYLE** column in "T_BADGES table" on page 58.
ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.
L_ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

V_GC_CUSTOM view

The V_GC_CUSTOM[4] view provides information for groups in the access catalog that use custom join in the provisioning policy.

Table 110. V_GC_CUSTOM view

Column Name	Description
ID	See the **entity_id** column in "T_AccessCatalog table" on page 56.
NAME	See the **name** column in "T_AccessCatalog table" on page 56.
L_NAME	See the **name** column in "T_AccessCatalog table" on page 56.
DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
L_DESCRIPTION	See the **description** column in "T_AccessCatalog table" on page 56.
CATEGORY	See the **Category** column in "T_AccessCatalog table" on page 56.
VIEW_OPTION	See the **view_option** column in "T_AccessCatalog table" on page 56.
ICON_URL	See the **icon_url** column in "T_AccessCatalog table" on page 56.
DN	See the **dn** column in "T_GROUP table" on page 58.
PROFILE	See the **Type** column in "T_GROUP table" on page 58.
BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
L_BU_DN	See the **BU_DN** column in "SA_EVALUATION_SERVICE table" on page 48.
RDN	See the **rdn_attr** column in "T_GROUP_PROFILE table" on page 63.
SERVICE_DN	See the **DN** column in "SA_EVALUATION_SERVICE table" on page 48.
SERVICE_ID	See the **ID** column in "SA_EVALUATION_SERVICE table" on page 48.
ACCT_ATTR	See the **acct_attr** column in "T_GROUP_PROFILE table" on page 63.
CASE_SENSITIVITY	See the **case_sensitivity** column in "T_GROUP_PROFILE table" on page 63.
TAG	See the **tag** column in "T_AccessCatalogTags table" on page 57.
L_TAG	See the **tag** column in "T_AccessCatalogTags table" on page 57.
BADGE_TEXT	See the **BADGE_TEXT** column in "T_BADGES table" on page 58.
BADGE_STYLE	See the **BADGE_STYLE** column in "T_BADGES table" on page 58.
ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.
L_ADDITIONALINFO	See the **additionalinfo** column in "T_AccessCatalog table" on page 56.

[4] Indicates that the view is added in IBM Security Identity Manager 6.0.0.2.

Database views tables

The tables described in this section are used for database views.

PENDING_APPROVAL view

This view is used in the design of Pending Approvals report. This view provides information about the process ID of a process with pending work items and the associated status.

Table 111. PENDING_APPROVAL view

Column Name	Description	Data type
PROCESSID	ID of the parent process for which there exists a pending work item.	Numeric
RESULT_SUMMARY	Actual status of the pending work item. Valid values for this column are: PE: The work item has some pending manual action from a workflow participant. ES: The work item was escalated to an escalation participant. LK: The work item was locked by a workflow participant.	Character

ROOTPROCESSVIEW view

This view is used in the design of Account operations and Account operations by individual report. The ROOTPROCESSVIEW captures all root processes, their IDs, types, and requestor information from PROCESS table. It is an SQL view defined on PROCESS table.

Table 112. ROOTPROCESSVIEW view table

Column Name	Description	Data type
ID	ID of the parent process initiated for am Security Identity Manageroperation.	Numeric
TYPE	ID of the parent process initiated for am Security Identity Manager operation.	Character
REQUESTER	The DN of the user who requested this process. PROCESS (REQUESTER).	Character

SUBPROCESSVIEW view

This view is used in the design of Account operations and Account operations by individual report. This view provides information about the subprocesses that are initiated due to various root processes. These processes are in turn initiated for different operations in the Security Identity Manager system.

Table 113. SUBPROCESSVIEW view table

Column Name	Description	Data type
ROOT_PROCESS_ID	ID of the parent process initiated for an Security Identity Manager operation.	Numeric
SUBMITTED	Time that the subprocess was submitted.	Numeric
COMPLETED	Time that the subprocess is completed.	Numeric
SUBJECT_PROFILE	Profile name of the subject.	Character
SUBJECT_SERVICE	ITIM service name.	Character
SUBJECT	Process subject.	Character

Table 113. SUBPROCESSVIEW view table (continued)

Column Name	Description	Data type
RESULT_SUMMARY	Process result summary code. Values include: Approved (AA) Rejected (AR) Submitted (RS) Success (SS) Timeout (ST) Failed (SF) Warning (SW) Pending (PE) Participant Resolution Failed (PF) Escalated (ES) Skipped (SK)	Character
TYPE	Type of the subprocess. Values include: Account Add (OA) Account Change (OC) Account Password Change (AP) Suspend Account (AS) Restore Account (AR) Delete Account (AD)	Character
REQUESTER	The DN of the user who requested this process.	Character

SUSPENDED_USERS view

The SUSPENDED_USERS[1] view is used in the design of Suspended Users report. This view provides the completion time of latest user suspend operation for a requestee.

Table 114. SUSPENDED_USERS view table

Column Name	Description	Data type
REQUESTEE	DN of the requestee.	Character
COMPLETED	Completion time of latest suspend operation for a requestee.	Character

[1] Indicates the view is added in release 4.6 Express.

SUSPENDED_ACCOUNT_OPERATIONS view

The SUSPENDED_ACCOUNT_OPERATIONS[1] view is used in the design of Suspended Accounts report. This view provides information about suspended account operation for each requestee. It is an SQL view defined on PROCESS table.

Table 115. SUSPENDED_ACCOUNT_OPERATIONS view table

Column Name	Description	Data type
REQUESTEE	DN of the requestee.	Character
SUBJECT_SERVICE	If the subject is an account, this field contains the name of the service associated with the account.	Character
SUBJECT	The subject of the process.	Character
SUBJECT_PROFILE	The data service object profile name that indicates the type of the subject.	Character
COMPLETED	Completion time of the latest suspended account operation for a requestee.	Character

[1] Indicates the view is added in release 5.0.

PROCESS_VIEW view

The PROCESS_VIEW[1] view is used in the design of Operations Report, User Report, and Rejected Report. This view is defined on PROCESS table.

Table 116. PROCESS_VIEW view table

Column Name	Description	Data type
ID	ID of the process.	Numeric
REQUESTER	DN of the requester.	Character
REQUESTEE	DN of the requestee.	Character

[1] Indicates the view is added in release 5.0.

Separation of duty policy tables

The tables described in this section are used for storing information about separation of duty policies and violations.

SOD_OWNER table

The SOD_OWNER[1] table stores information about the owners for a separation of duty policy. There can be more than one owner for each separation of duty policy.

Table 117. SOD_OWNER table

Column Name	Description	Data type
ID*	Owner unique ID. Primary key.	Numeric
POLICY_ID*	Separation of duty policy ID that is associated with the data. References SOD_POLICY(ID).	Numeric
OWNER_NAME	Name of the person or role that is listed as the owner of this separation of duty policy.	Character (256)
BUSINESS_UNIT_NAME	Name of the business unit of the person or role defined in OWNER_NAME.	Character (256)
TYPE	The type of owner represented by this row. Valid values are: Person (P) Role (R)	Character (2)

Table 117. SOD_OWNER table (continued)

Column Name	Description	Data type
DN	DN to the owner specified in the IBM Security Identity Manager LDAP store.	Character (2000)

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

SOD_POLICY table

The SOD_POLICY[1] table stores information about a separation of duty policy. This table is used by the inner workings of separation of duty implementation and separation of duty reports.

Table 118. SOD_POLICY table

Column Name	Description	Data type
ID*	Separation of duty policy unique ID. Primary key.	Numeric
GLOBAL_ID*	The global identifier of this separation of duty policy in LDAP.	Numeric
NAME	Name of this separation of duty policy.	Character (256)
DESCRIPTION	Description of this separation of duty policy.	Character (500)
BUSINESS_UNIT_NAME	Name of the business unit for this separation of duty policy.	Character (256)
ENABLED	The state of the separation of duty policy. Valid values are: Enabled (T) Disabled (F) Deleted (D)	Character (1)
DN	DN to this separation of duty policy as specified in the IBM Security Identity Manager LDAP store.	Character (2000)
VERSION*	Timestamp for when this policy was written to the database. It might happen through policy add/modify/delete/evaluate.	Numeric

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

SOD_RULE table

The SOD_RULE[1] table stores information about a separation of duty policy rule. This table is used by the inner workings of separation of duty implementation and separation of duty reports.

Table 119. SOD_RULE table

Column Name	Description	Data type
ID*	Separation of duty policy rule unique ID. Primary key.	Numeric
POLICY_ID*	Separation of duty policy ID that is associated with the data. References SOD_POLICY(ID).	Numeric
GLOBAL_ID*	The global ID of this separation of duty policy rule in LDAP.	Numeric
NAME	Name of this separation of duty policy rule.	Character (500)

Table 119. SOD_RULE table (continued)

Column Name	Description	Data type
DESCRIPTION	Description of this separation of duty policy rule.	Character (500)
CARDINALITY	Allowed number of roles defined for this policy rule.	Numeric
VERSION*	Timestamp for when this policy rule was written to the database. It might happen through policy add, modify, delete, and evaluate.	Numeric

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

SOD_RULE_ROLE table

The SOD_RULE_ROLE[1] table stores information about the roles listed in a separation of duty policy rule. This table is used by the inner workings of separation of duty implementation and separation of duty reports.

Table 120. SOD_RULE_ROLE table

Column Name	Description	Data type
ID*	Separation of duty policy rule unique ID. Primary key.	Numeric
POLICY_RULE_ID*	Separation of duty policy rule ID that is associated with the data. References SOD_RULE(ID).	Numeric
GLOBAL_ID*	The global identifier of this role in LDAP.	Numeric
NAME	Name of this role.	Character (256)
DESCRIPTION	Description of this role.	Character (500)
BUSINESS_UNIT_NAME	Name of the business unit for this role.	Character (100)
DN	DN to this role as specified in the IBM Security Identity Manager LDAP store.	Character (2000)

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

SOD_VIOLATION_HISTORY table

The SOD_VIOLATION_HISTORY[1] table stores historical information about exemptions and violations for a separation of duty policy.

Table 121. SOD_VIOLATION_HISTORY table

Column Name	Description	Data type
ID*	Unique ID for this historical record of separation of duty violation. Primary key.	Numeric
POLICY_GLOBAL_ID*	The global identifier of the separation of duty policy in LDAP to which this record refers.	Numeric
RULE_GLOBAL_ID*	The global identifier of the separation of duty policy rule in LDAP to which this record refers.	Numeric
PERSON_GLOBAL_ID*	The global identifier of the person to which this violation refers in LDAP.	Numeric
PERSON_NAME	Name of the person to which this violation refers.	Character (256)
PERSON_BU	Name of the business unit for the person in PERSON_DN.	Character (256)

Table 121. SOD_VIOLATION_HISTORY table (continued)

Column Name	Description	Data type
PERSON_DN	DN to the person record as specified in the IBM Security Identity Manager LDAP store.	Character (2000)
PROCESS_ID	The associated workflow process ID that changed the state of this violation. It might not have a value if the violation was discovered by policy evaluation or exemption administration through the administrative console.	Numeric
ADMIN_NAME	Name of the person who revoked or exempted this violation.	Character (256)
ADMIN_BU	Name of the business unit for the person in ADMIN_DN.	Character (256)
ADMIN_DN	DN to the person record who revoked or exempted this violation as specified in the IBM Security Identity Manager LDAP store.	Character (2000)
ADMIN_NOTES	Justification notes (text) that the person in column ADMIN_DN entered at time of revoke/exempt of violation.	Character
STATUS	The state of this historical record about a violation or exemption. Valid values are: Violation (V) Exemption (A) Revoked Exemption (R) No longer a violation (N)	Character (1)
TS*	Timestamp when the action recorded in this record occurred.	Numeric

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

SOD_VIOLATION_STATUS table

The SOD_VIOLATION_STATUS[1] table stores current information about exemptions and violations for a separation of duty policy.

Table 122. SOD_VIOLATION_STATUS table

Column Name	Description	Data type
ID*	Unique ID for this record of separation of duty violation. Primary key.	Numeric
POLICY_GLOBAL_ID*	The global identifier of the separation of duty policy in LDAP to which this record refers.	Numeric
RULE_GLOBAL_ID*	The global identifier of the separation of duty policy rule in LDAP to which this record refers.	Numeric
PERSON_GLOBAL_ID*	The global identifier of the person to which this violation refers in LDAP this record.	Numeric
PERSON_NAME	Name of the person to which this violation refers.	Character (256)
PERSON_BU	Name of the business unit of the person in PERSON_DN.	Character (256)
PERSON_DN	DN to the person record as specified in the IBM Security Identity Manager LDAP store.	Character (2000)

Table 122. SOD_VIOLATION_STATUS table (continued)

Column Name	Description	Data type
PROCESS_ID	The associated workflow process ID that changed the state of this violation. It might not have a value if the violation was discovered by policy evaluation or exemption administration through the administrative console.	Numeric
ADMIN_NAME	Name of the person who revoked or exempted this violation.	Character (256)
ADMIN_BU	Name of the business unit of the person in ADMIN_DN.	Character (256)
ADMIN_DN	DN to the person record who revoked or exempted this violation as specified in the IBM Security Identity Manager LDAP store.	Character (2000)
ADMIN_NOTES	Justification notes (text) that the person in column ADMIN_DN entered at time of revoke/exempt of violation.	Character
STATUS	The state of this record about a violation or exemption. Valid values are: Violation (V) Exemption (A)	Character (1)
TS*	Timestamp when the action recorded in this record occurred.	Numeric
EVAL_TS*	Timestamp when this violation was last known to be true during sod policy evaluation.	Numeric

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

SOD_VIOLATION_ROLE_MAP table

The SOD_VIOLATION_ROLE_MAP[1] table stores information about the roles that are involved in a violation. The roles on the person that are part of a violation are mapped to the roles in the policy rule.

Table 123. SOD_VIOLATION_ROLE_MAP table

Column Name	Description	Data type
ID*	Unique ID for this record. Primary key.	Numeric
VIOLATION_ID*	Separation of duty violation ID that is associated with the data. References SOD_VIOLATION_STATUS(ID) and SOD_VIOLATION_HISTORY(ID).	Numeric
RULEROLE	The DN of the role as referenced in the separation of duty policy rule that is involved in this violation.	Character (2000)
PERSONROLE	The DN of the role on the person that is found to be in violation of the separation of duty policy rule.	Character (2000)

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.1.

Others

This section describes other tables.

ACI_CATEGORIES table

The ACI_CATEGORIES[3] stores the access control protection categories.

Table 124. ACI_CATEGORIES table

Column Name	Description	Data type
ID*	The unique ID of the ACI category.	Numeric
NAME*	The ACI category name. Primary key.	Character (255)

* Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

AUTH_KEY table

The AUTH_KEY table stores the keys for signing and verifying authentication requests.

Table 125. AUTH_KEY table

Column Name	Description	Data type
Y*	The public key in the DSA algorithm.	Character (2000)
P*	The prime number in the DSA algorithm.	Character (2000)
Q*	The subprime number in the DSA algorithm.	Character (2000)
G*	The modulus in the DSA algorithm.	Character (2000)
X*	The private key in the DSA algorithm.	Character (2000)

* Indicates the column is required and not null.

COMMON_TASKS table

The COMMON_TASKS[1] table stores common tasks for each persona.

Table 126. COMMON_TASKS table

Column Name	Description	Data type
PERSONA*	Name of the persona. Primary key.	Character (100)
TASK_ID*	Unique ID of a task. Primary key. References TASKS_VIEWABLE (TASK_ID).	Character (255)

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.0.

LCR_INPROGRESS_TABLE table

LCR_INPROGRESS_TABLE tracks the lifecycle rule that is in progress for a particular entity. This table prevents two or more lifecycle rules from operating on the same entity at any time.

Table 127. LCR_INPROGRESS_TABLE table

Column Name	Description	Data type
TENANT*	The name of the tenant for which the lifecycle rule applies.	Character (256)
RULE_ID*	Identifier for the lifecycle rule.	Numeric

Table 127. LCR_INPROGRESS_TABLE table (continued)

Column Name	Description	Data type
RULE_OP	Operation for the lifecycle rule.	Character (256)
CHILD_ID	Identifier for the child process of the lifecycle rule.	Numeric
START_TIME	Time when the child process started.	Numeric
ENTITY_ID*	Identifier of the entity on which this lifecycle rule operation is in progress.	Character (256)

* Indicates the column is required and not null.

ROLE_INHERITANCE table

The ROLE_INHERITANCE[1] table stores the relationships between roles in the role hierarchy.

Table 128. ROLE_INHERITANCE table

Column Name	Description	Data type
ASCENDENT	The DN of the parent role in this parent-child relationship.	Character (2000)
DESCENDENT	The DN of the child role in this parent-child relationship.	Character (2000)

[1] Indicates the table is added in release 5.1.

SCHEDULED_MESSAGE table

The SCHEDULED_MESSAGE table stores information associated with a scheduled event that is provided by the scheduler. The scheduler is a component of IBM Security Identity Manager that stores one-time or regularly scheduled events. These events are typically user requests that are made through the workflow engine or recurring reconciliation events.

Table 129. SCHEDULED_MESSAGE table

Column Name	Description	Data type
SCHEDULED_TIME	A value that represents the time of the scheduled event, which is the number of milliseconds since January 1, 1970, 00:00:00 Greenwich mean time.	Numeric
SCHEDULED_MESSAGE_ID*	Unique ID for each scheduled event. Primary key.	Numeric
MESSAGE	A serialized object that represents the detailed information about the scheduled event.	Long Character
SMALL_MESSAGE[1]	A small serialized object that represents the detailed information about the scheduled event.	Character (4000)
SERVER	The server that picks up the most recently scheduled event.	Character (255)
CHECKPOINT_TIME	A value that represents the last pickup time of the scheduled event, which is the number of milliseconds since January 1, 1970, 00:00:00 Greenwich mean time.	Numeric
REFERENCE_ID	Used only for scheduled workflow events, it is the workflow process ID from which the scheduled event is coming.	Numeric
REFERENCE_ID2	Used to store label and meta information about the scheduled message.	Numeric

* Indicates the column is required and not null.

[1] Indicates the table is added in release 5.0.

TASK_TREE table

The TASK_TREE[3] stores the master task IDs and the task tree structure information from **Set System Security** > **Manage Views** in the IBM Security Identity Manager Console.

Table 130. TASK_TREE table

Column Name	Description	Data type
PARENT	The unique ID of the parent task.	Character (500)
TASK_ID*	The unique ID of the task. Primary key.	Character (500)
SEQUENCE_NO	The sequence number of the task for ordering purpose.	Numeric
ADMIN_ONLY	The flag indicates whether the task is exposed from **Set System Security** > **Manage Views** in the IBM Security Identity Manager Console. Values include: • Y – not exposed and therefore not configurable. • N – exposed and configurable for each view.	Character (1)

[*] Indicates the column is required and not null.

[3] Indicates the table is added in IBM Security Identity Manager 6.0.

TASKS_VIEWABLE table

The TASKS_VIEWABLE[1] table stores task settings for each view. The information determines which tasks are available and enabled in a view.

Table 131. TASKS_VIEWABLE table

Column Name	Description	Data type
TASK_ID*	Unique ID of a task. Primary key.	Numeric
VIEW_ID	Unique ID of a view definition. References VIEW_DEFINITION (ID).	Numeric
VIEWABLE	To determine whether a task is enabled for in a view. Values: 'Y' or 'N'.	Character (1)

[*] Indicates the column is required and not null.

[1] Indicates the table is added in release 5.0.

VIEW_DEFINITION table

The VIEW_DEFINITION[1] table stores view definitions. The information is used to create, modify, delete, and search views.

Table 132. VIEW_DEFINITION table

Column Name	Description	Data type
ID*	Unique ID of a view definition. Primary key.	Numeric
NAME	Name of a view definition.	Character (100)
DESCRIPTION	Description of a view definition.	Character (2000)

[*] Indicates the column is required and not null.

[1] Indicates the table is added in release 5.0.

Chapter 2. IBM Security Directory Server schema and class reference

This section provides descriptions about the IBM Security Identity Manager directory information tree and the classes it uses in the Security Directory Server.

IBM Security Identity Manager directory tree

This section describes the Security Identity Manager directory tree.

The following is a diagram of a basic Security Identity Manager directory tree:

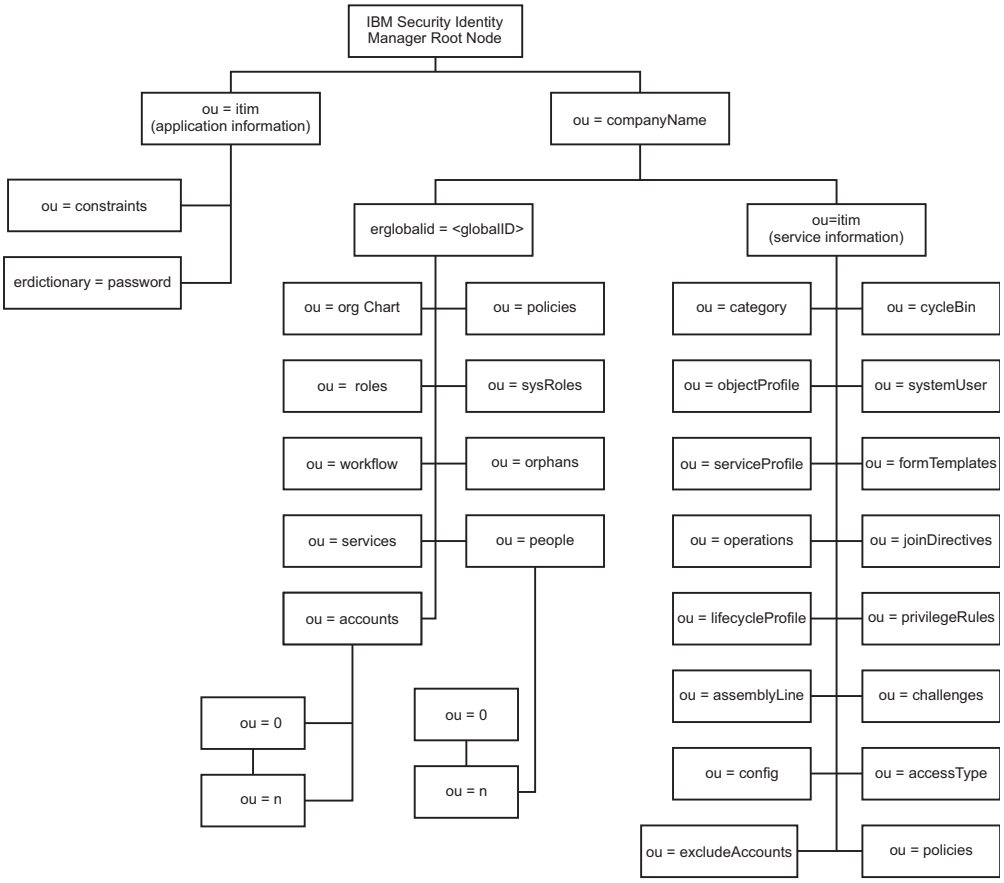

Table 133. Brief descriptions of each container in the directory tree

Container	Description
`Root Node`	Root node where the IBM Security Identity Manager Server is installed.
`ou=itim`	This container stores all pertinent information for the Security Identity Manager application.
`ou=constraints`	This container stores membership restrictions for various roles and services.
`erdictionaryname=password`	This container stores invalid password entries for use with password policies.
`ou=`*`CompanyName`*	Name of the company. This container is the parent container for all information about the company in the Security Identity Manager system.

Table 133. Brief descriptions of each container in the directory tree (continued)

Container	Description
erglobalid=<GlobalID>	This node stores information of the organization. The company long name can be found in this node.
ou=orgChart	This container stores the definition of the organizations and organizational units in Security Identity Manager.
ou=roles	This container stores all information for all organizational roles defined in Security Identity Manager.
ou=workflow	This container stores all the workflows designed for use in the Security Identity Manager system for the company.
ou=services	This container stores information about the services installed for use with the Security Identity Manager system.
ou=accounts	This container stores all accounts in the Security Identity Manager system.
ou=policies	This container stores all the defined policies.
ou=sysRoles	This container stores all information about the Security Identity Manager Groups defined in Security Identity Manager.
ou=orphans	This container stores all orphan accounts retrieved during reconciliation.
ou=people	This container stores all information about Persons in Security Identity Manager.
ou=credCatalog[2]	This container stores information about credentials and credential pools
ou=itim	This container is the parent container for system-specific information.
ou=category	This container stores lifecycle management operations for an entity type. Only Person and Account are supported. Global represents the system operation.
ou=objectProfile	This container stores the object profiles required for the system to recognize a managed resource as an entity (person, organizational unit, location).
ou=serviceProfile	This container stores the service profiles required for the system to recognize a managed resource as a service.
ou=operations	This container stores information about workflow operations (such as add, modify, delete, suspend, and transfer) with Security Identity Manager.
ou=lifecycleProfile	This container stores all information about the lifecycle characteristics that are defined at the entity (instance) level.
ou=assemblyLine	This container stores all information about the configuration for the service IDI adapter.
ou=config	This container stores all the information about the workflow configurations.
ou=excludeAccounts	This container stores all the information about which accounts are to be excluded during reconciliation.
ou=recycleBin	This container stores entities deleted from the system by the administrative console.
ou=systemUser	This container stores information about system users.
ou=formTemplates	This container stores information about the various forms and the form templates used in the system.
ou=joinDirectives	This container stores all the information about the provisioning policy join directives.
ou=privilegeRule	This container stores information that determines whether the difference between an account value and what is dictated by a provisioning policy requires revoking or granting privileges.
cn=challenges	This container stores all information about the password challenge and response feature.
ou=accessType[1]	This container stores information about access types.

Table 133. Brief descriptions of each container in the directory tree (continued)

Container	Description
ou=policies[1]	This container stores information about account defaults for each service.
ou=ownershipType[2]	This container stores information about ownership types.

[1] Indicates that the container is added in Version 5.0.

[2] Indicates that the container is added in Version 6.0

General classes

The IBM Security Identity Manager system uses the directory server default schema and a specific schema.

The Security Identity Manager schema consists of a collection of auxiliary classes that provide the interface necessary to run its system business logic. These auxiliary classes can be used with custom-defined classes to complete the schema used by Security Identity Manager . The following classes listed are default classes that are managed by Security Identity Manager. An additional term to note is:

Domain entry
An entry in the directory that corresponds to a business entity managed by Security Identity Manager.

erBPPersonItem

The erBPPersonItem class is an auxiliary class that identifies attributes for a IBM Business Partner person. This class is a domain entry. The parent class is top.

Table 134. erBPPersonItem table

Attribute name	Description	Type
Mail	Email address.	directory string
Cn	Common name for person.	directory string
erPersonStatus	Status of person.	integer
erSponsor	DN of sponsor for this person.	distinguished name
erRoles	DN of roles for person.	distinguished name
erAliases	Aliases for person.	directory string
erSharedSecret	Value used by the user for password pickup.	directory string
erCustomDisplay	User-selected attribute to display in the BP Person list.	directory string
erLocale	The locale preference of the user. Default is the system locale.	directory string
erCreateDate	Timestamp of when the object is created. The timestamp is in Greenwich Mean Time format.	directory string
erSynchPassword	Password to be used for account creation.	binary
erLastStatusChangeDate	Timestamp of when the status is updated. The timestamp is in Greenwich Mean Time format.	directory string
erLastOperation	Available for custom use for lifecycle event.	directory string

Table 134. erBPPersonItem table (continued)

Attribute name	Description	Type
erPswdLastChanged	Timestamp of the last password change date. The timestamp is in Greenwich Mean Time format.	generalized time
erLastCertifiedDate[1]	Timestamp of the last execution of a user recertification policy for this user. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the policy definition, and the second part is the timestamp of the policy implementation.	directory string
erRoleRecertificationLastAction[2]	The last recertification action applied to a role membership. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the role definition, and the second part is the last action applied to the role membership. Valid actions are: Certified (CERTIFIED) Rejected and marked (REJECTED_MARK)	directory string
erRoleRecertificationLastActionDate[2]	Timestamp of the last recertification action applied to a role membership. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the role definition, and the second part is the timestamp of the last action.	directory string
erPersonPassword[1]	Account password of the person.	directory string
erRoleAssignments[3]	Represents the person role assignment attribute value information. A multi-valued attribute that contains ";;" delimited strings. The first part of each string is the DN of the role definition. The second part is the assignment attribute name. The third part is the assignment attribute value.	directory string
erURI[3]	The universal resource identifier.	directory string

[1] Indicates the attribute is added in release 4.6 Express.

[2] Indicates the attribute is added in release 5.1.

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erBPOrg

The erBPOrg class is a structural class that stores business partner organization information. This class is a domain entry. The parent class is top.

Table 135. erBPOrg table

Attribute name	Description	Type
ou	Organizational unit. This attribute is required.	directory string
description	Description of the business partner organization.	directory string

erBPOrgItem

The erBPOrgItem class is an auxiliary class that stores business partner (BP) organization information. This class is a domain entry. The parent class is top.

Table 136. erBPOrgItem table

Attribute name	Description	Type
ou	Organizational unit name.	directory string
erBPOrgStatus	Status of the BP organization.	integer
erSponsor	DN of organizational unit supervisor.	distinguished name
erURI[3]	The universal resource identifier.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erDictionary

The erDictionary class stores words that cannot be used as passwords. This class is a domain entry. The parent class is top.

Table 137. erDictionary table

Attribute name	Description	Type
erDictionaryName	The name of the dictionary. This attribute is required.	directory string
description	Description of the dictionary.	directory string

erDictionaryItem

The erDictionaryItem class stores an individual word that is not allowed as a password. These classes are then linked together with the erDictionary class. This class is a domain entry. The parent class is top.

Table 138. erDictionaryItem table

Attribute name	Description	Type
erWord	The word that is excluded from being used as a password. This attribute is required.	directory string
description	Description of the word and the reason it cannot be used as a password.	directory string

erDynamicRole

The erDynamicRole class provides the structure for a dynamic role. The parent class is erRole.

Table 139. erDynamicRole table

Attribute name	Description	Type
erJavaScript	Role evaluation definition. This definition is used to evaluate members of a role.	binary
erScope	Scope of role evaluation: single or subtree scope.	integer

erFormTemplate

The erFormTemplate class stores form template information. This class is a domain entry. The parent class is top.

Table 140. erFormTemplate table

Attribute name	Description	Type
erFormName	The name of the form. This attribute is required.	directory string
erCustomClass	Name of the entity class.	directory string
erXML	The actual XML code for the form.	binary

erIdentityExclusion

The erIdentityExclusion class stores the names of the accounts that are not retrieved during reconciliation. This class is a domain entry. The parent class is top.

Table 141. erIdentityExclusion table

Attribute name	Description	Type
cn	Common name. This attribute is required.	directory string
erObjectProfileName	Service profile name.	directory string
erAccountID	Account ID to exclude from the reconciliation.	directory string

erLocationItem

The erLocationItem class is an auxiliary class that stores attributes of a location within the system. The location name attribute must be defined. The erLocationItem class is a domain entry and includes the erManagedItem class. The parent class is top.

Table 142. erLocationItem table

Attribute name	Description	Type
l	Location name. This attribute is required.	directory string
erSupervisor	DN of location supervisor.	distinguished name
erURI[3]	The universal resource identifier.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erManagedItem

The erManagedItem class is an auxiliary class that is added to all domain entries (organizations, organizational units, people, and roles) that require access control. The erManagedItem class defines a unique ID, a parent entry (if present), and an access control list. The parent class is top.

Table 143. erManagedItem table

Attribute name	Description	Type
erGlobalId	Unique, random ID assigned to all entries in a directory. Used as the regional DN for each entry.	number string
erLastModifiedTime	Entry removal date and time (GMT format).	directory string
erAcl	Access control list.	binary

Table 143. erManagedItem table (continued)

Attribute name	Description	Type
erAuthorizationOwner	Owner of access control.	distinguished name
erParent	Entry organizational unit DN.	distinguished name
erIsDeleted	True, if in recycle bin.	directory string
erLifecycleEnable	Specifies whether the lifecycle operation is defined on an entity. If true, there is a lifecycle operation defined for an entity.	Boolean
erProfileName	Profile name of an object.	directory string
erURI[1]	Universal resource identifier of an object.	case exact matching string

[1] Indicates the attribute is added in Version 6.0.

erOrganizationItem

The erOrganizationItem class is an auxiliary class that is added to organizations. The erOrganizationItem class is a domain entry and includes the erManagedItem class. It defines the organization name and status. The parent class is top.

Table 144. erOrganizationItem table

Attribute name	Description	Type
o	Organization name.	directory string
erOrgStatus	Organization status.	integer
erURI[3]	The universal resource identifier.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erOrgUnitItem

The erOrgUnitItem class is an auxiliary class that stores information about an organizational unit. It contains information about the ou name and optionally the supervisor (erSupervisor) for an organizational unit. The erOrgUnitItem is a domain entry. The parent class is top.

Table 145. erOrgUnitItem table

Attribute name	Description	Type
ou	Organizational unit.	directory string
erSupervisor	DN of organizational unit supervisor.	distinguished name
erURI[3]	The universal resource identifier.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erPersonItem

The erPersonItem class is an auxiliary class that identifies attributes for a person. The erPersonItem is a domain entry. The parent class is top.

Table 146. erPersonItem table

Attribute name	Description	Type
Mail	Email address.	directory string
Cn	Common name for person.	directory string
erPersonStatus	Status of person.	integer
erRoles	DN of the roles of the person.	distinguished name
erAliases	Aliases for person.	directory string
erSupervisor	DN of the supervisor of the person.	distinguished name
erSharedSecret	Value used by the user for password pickup.	directory string
erCustomDisplay	User-selected attribute to display in Person lists.	directory string
erLocale	Locale preference of the user. Default is the system locale.	directory string
erCreateDate	Timestamp of when the object is created. The timestamp is in Greenwich Mean Time (GMT) format.	directory string
erSynchPassword	Password to be used for account creation.	binary
erLastStatusChangeDate	Timestamp of when the status is updated. The timestamp is in GMT format.	directory string
erLastOperation	Available for custom use for lifecycle event.	directory string
erPswdLastChanged	Timestamp of the last password change date. The timestamp is GMT format.	generalized time
erLastCertifiedDate[1]	Timestamp of the last execution of a user recertification policy for this user. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the policy definition, and the second part is the timestamp of the policy execution.	directory string
erRoleRecertificationLastAction[2]	The last recertification action applied to a role membership. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the role definition, and the second part is the last action applied to the role membership. Valid actions are: Certified (CERTIFIED) Rejected and marked (REJECTED_MARK)	directory string
erRoleRecertificationLastActionDate[2]	Timestamp of the last recertification action applied to a role membership. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the role definition, and the second part is the timestamp of the last action.	directory string
erPersonPassword[1]	Account password of the person.	directory string
erRoleAssignments[3]	Represents the person role assignment attribute value information. A multi-valued attribute that contains ";;" delimited strings. The first part of each string is the DN of the role definition. The second part is the assignment attribute name. The third part is the assignment attribute value.	directory string
erURI[3]	The universal resource identifier.	directory string

[1] Indicates the attribute is added in release 4.6 Express.

[2] Indicates the attribute is added in release 5.1.

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erRole

The erRole class stores the name and description for an organizational role. However, it does not store membership information. The user membership is stored in erPersonItem.erRoles, and the role membership is stored in the ROLE_INHERITANCE database table. This class is a domain entry. The parent class is top.

Table 147. erRole table

Attribute name	Description	Type
erRoleName	Name of the organizational role. This attribute is required.	directory string
description	Description of the role.	directory string
erSubRoles[1]	Contains no value, attribute is used for ACI permission on managing child roles.	directory string
erRoleClassification[1]	The classification of role, application role, system role, and others.	directory string
owner[1]	The owner of the role, can be person dn or role dn.	distinguished name
erRoleAssignmentKey[3]	The assignment attributes of a role (multi-valued attribute).	directory string
erURI[3]	The universal resource identifier.	directory string

[1] Indicates the attribute is added in release 5.1.

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erSecurityDomainItem

The erSecurityDomainItem class is an auxiliary class for an admin domain. The parent class is top.

Table 148. erSecurityDomainItem table

Attribute name	Description	Type
ou	Organizational unit.	directory string
erAdministrator	DN of the administrator of an admin domain.	distinguished name
erURI[3]	The universal resource identifier.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

SecurityDomain

The SecurityDomain class stores admin domain information. This class is a domain entry. The parent class is top.

Table 149. `SecurityDomain` table

Attribute name	Description	Type
`ou`	Organizational unit. This attribute is required.	directory string
`description`	Description of the admin domain.	directory string

erTemplate

The `erTemplate` class stores notification template information. This class is a domain entry. The parent class is top.

Table 150. `erTemplate` table

Attribute name	Description	Type
`cn`	Either name or global ID of the notification template.	directory string
`erEnabled`	Specifies whether the notification template is enabled.	Boolean
`erTemplateName`[1]	Name of the notification template.	directory string
`erSubject`	Content in the subject field of the notification.	binary
`erText`	Content in the text field of the notification.	binary
`erXHTML`	Content in the XHTML field of the notification.	binary
`erType`[1]	Type of the notification template. Values include: 0 – Undefined 1 – Recertification Approval 2 – Recertification Work Order 3 – Mail Template 4 – User Recertification Approval[2] 5 – User Recertification Work Order[2]	directory string
`erIsReadOnly`[1]	Specifies whether the notification template is read-only. If it is read-only, the user cannot modify the content of the notification template.	Boolean

[1] Indicates the attribute is added in release 4.6 Express.

[2] Indicates the attribute value is added in release 5.1.

erTenant

The `erTenant` class defines properties based on a tenant, such as the `ou` if passwords can be edited or lost passwords can be mailed. The parent class is top.

Table 151. erTenant table

Attribute name	Description	Type
ou	Organization unit that contains this tenant. This attribute is required.	directory string
erIsActive	Indicates whether this tenant is active. This attribute is required.	Boolean
description	Description of tenant.	directory string
erPswdEditAllowed	Indicates whether passwords might be set (true) or generated (false). This attribute is required.	Boolean
erLostPswdByMail	Indicates whether passwords can be mailed to a user for this tenant. This attribute is required.	Boolean
erBucketCount	Hash bucket number. This attribute is required.	integer
erLastModifiedTime	Time the tenant was last modified (attributes).	directory string
erPswdExpirationPeriod	Number of days after which the password becomes expired. When the user tries to access the system after the password expires, the user is forced to change the password. When this value is set to 0, the password does not expire.	integer
erPswdTransactionExpPeriod	Number of hours after which the transaction to retrieve an account password expires. The password is typically retrieved with the URL link provided in an email message from the system. When this value is set to 0, the URL link does not expire.	integer
erLogonCount	Number of invalid login attempts that the user can have before the user account is suspended. When this value is set to 0, the user can attempt to access the system without limit, and the system does **not** suspend the account.	integer
erResponseEnable	Attribute for enabling or disabling the password challenge and response feature. When this attribute is set to TRUE, the user can use the **Forgot Your Password** link to enter the system by providing correct answers to the password challenge and response questions.	Boolean
erResponseDescription	Message on the login page when the user account is suspended after the user • Tries to log in to the system too many times. • Fails to respond correctly to the password challenge and response questions.	directory string
erResponseEmail	Message emailed to the administrator responsible for user accounts suspended when the user fails to access the system in the defined number of tries.	directory string

Table 151. erTenant table (continued)

Attribute name	Description	Type
erChallengeMode	Password Challenge Response mode. The following modes are available: PRE-DEFINED: When this mode is selected, the user must correctly answer all the challenge questions that are defined by the system administrator to access the system. USER-SELECTED: When this mode is selected, the user must correctly answer the challenge questions selected when the challenge/response feature for the account was configured. The challenge questions are selected from a defined list. RANDOM-SELECTED: When this mode is selected, the user must correctly answer the challenge questions selected by the system. The challenge questions are randomly selected from a defined list.	directory string
erRequiredChallenges	Number of challenges to which the user must correctly respond to access the system when the password is forgotten.	integer
erRandomChallenges	Number of challenges available from which the system can select for password challenge and response questions to users who forgot their passwords.	integer
erHashedEnabled	Not used.	Boolean
erRespLastChange	Timestamp of when the administrator last changed the Password Challenge/Response configuration.	generalized time
erChallengeDefMode	Definition mode for lost password challenge response. Possible values are: Admin Defined (0) User Defined (1)	integer
erPswdSyncAllowed	Attribute for enabling and disabling password synchronization for user accounts.	Boolean
erNonComplianceAction	Compliant action for accounts of the service. Possible values are: Mark NonCompliant (0) Suspend NonCompliant (1) Correct NonCompliant (2) Use Workflow (3)	integer
erAlertOption	Option settings for when the compliance alert is triggered. Possible values are: Reconciliation (0) Policy change (1) Person data change (2) Account data change (3)	integer

Table 151. erTenant table (continued)

Attribute name	Description	Type
erShowGenPwd[1]	Indicates whether the generated password is displayed on the screen.	Boolean
erPwdEnabled[2]	Indicates whether password is enabled.	Boolean
erAutoGroupMembershipEnabled[2]	Indicates whether automatic group membership of certain IBM Security Identity Manager accounts is enabled.	Boolean

[1] Indicates the attribute is added in release 4.6 Express.

[2] Indicates the attribute value is added in release 5.0.

erWorkflowDefinition

The erWorkflowDefinition class stores workflow information. This class is a domain entry. The parent class is top.

Table 152. erWorkflowDefinition table

Attribute name	Description	Type
erProcessName	The name of the workflow. This attribute is required.	directory string
erObjectProfileName	Service profile name.	directory string
erXML	Definition of workflow.	binary
erCategory	Type of entity to manage, such as Person, BPPerson, or Account.	directory string
description[1]	Description of the workflow.	directory string

[1] Indicates the attribute value is added in release 5.0.

erOwnershipType

The erOwnershipType class is a structural class that represents an ownership type. The parent class is top.

Table 153. erOwnershipType table

Attribute name	Description	Type
erObjectProfileName	Name of the ownership type.	directory string
description	Description of the ownership type.	directory string

Service classes

Services can be hosted or owned. A hosted service is a service that is shared by multiple organizations, such as in an ASP environment. An owned service is not shared. Each type of service has its own, different representation in the system.

erAccessItem

The erAccessItem[1] class is an auxiliary class that defines required attributes for Access Entitlement. The parent class is top.

Table 154. erAccessItem table

Attribute name	Description	Type
erAccessName	Name of an access.	directory string
erObjectProfileName	Access types defined in the system. Default access types are: Role, Application, SharedFolder, MailGroup	directory string
erAccessOption	Access option. Values include: 1 – Access is disabled for user request 2 – Access is enabled for user request. 3 – Access is enabled for user request and it is commonly requested.	integer
erApprovalProcessID	DN pointed to the approval workflow that is used for access provisioning.	distinguished name
erNotifyAccessProvision	Indication whether a notification is sent when an access is granted to the user.	Boolean
erNotifyAccessDeprovision	Indication whether a notification is sent when an access is revoked from the user.	Boolean
erAccessDescription	Description of an access.	directory string
owner	DN of the access owner.	distinguished name

[1] Indicates the class is added in release 5.0.

erAccessType

The erAccessType[1] class is a structural class to represent an access type. The parent class is top.

Table 155. erAccessType table

Attribute name	Description	Type
erObjectProfileName	Name of the access type. This attribute is required.	directory string
description	Description of the access type.	directory string

[1] Indicates the class is added in release 5.0.

erAccountItem

The erAccountItem class is an auxiliary class that defines required attributes for a user account. The parent class is top.

Table 156. erAccountItem table

Attribute name	Description	Type
erUid	Account login ID.	directory string
Owner	DN of the account owner.	distinguished name
erAccountStatus	Account status.	integer

Table 156. erAccountItem table (continued)

Attribute name	Description	Type
erAccountCompliance	Compliancy of the account. Possible values are: Uncheck account (0) Compliant account (1) Unauthorized account (2) Constraints violated account (3)	integer
erPassword	Account login password.	binary
erPswdLastChanged	Date and time that the password was last changed.	generalized time
erHistoricalPassword	Previous account login password.	binary
erService	DN of the account service.	distinguished name
erLastAccessDate	Last login date.	generalized time
erPasswordLastChangedBy[4]	The DN of the person which last changed the password.	distinguished name
erCreateDate	Timestamp of when the object is created. The timestamp is in Greenwich Mean Time (GMT) format.	directory string
erLastStatusChangeDate	Timestamp of when the status is updated. The timestamp is in GMT format.	directory string
erLastOperation	Available for custom use for lifecycle event.	directory string
erLastCertifiedDate[1]	Timestamp of when the object was last certified.	directory string
erLastRecertificationAction[2]	The last recertification action applied to the account. Valid values are: Certified (CERTIFIED) Administrator override certified (CERTIFIED_ADMIN) Rejected and marked (REJECTED_MARK) Rejected and suspended (REJECTED_SUSPEND)	directory string
erLastRecertificationActionDate[3]	Timestamp of the last recertification action applied to the account.	directory string
erAccessLastCertifiedDate[2]	Timestamp of when the access was last certified. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the group definition associated with the access. The second part is the timestamp of when the access was last certified.	directory string

Table 156. erAccountItem table (continued)

Attribute name	Description	Type
erAccessRecertificationLastAction[2]	The last recertification action applied to a group or access. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the group definition. The second part is the last action taken on the group or access. Valid values are: Certified (CERTIFIED) Administrator override certified (CERTIFIED_ADMIN) Rejected and marked (REJECTED_MARK)	directory string
erAccessRecertificationLastActionDate[3]	Timestamp of the last recertification action applied to a group or access. A multivalued attribute that contains ";;" delimited strings. The first part of each string is the DN of the group definition. The second part is the timestamp of the last action.	directory string
erObjectType[2]	The value represents the type of the account. Predefined values are: 0 – user account 1 – system account	integer
erObjectProfileName	Name of the ownership type.	directory string
erAccountOwnershipType[4]	The account ownership type. If the value is not specified, it is interpreted as Individual account.	directory string
erURI[4]	The universal resource identifier.	directory string
erCVCatalog[4]	The DN of the credential if the account is added to the credential vault.	distinguished name

[1] Indicates the attribute is added in release 4.6 Express.

[2] Indicates the class is added in release 5.0.

[3] Indicates the class is added in release 5.1.

[4] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erADJNDIFeed

The erADJNDIFeed[1] class is a structural class and provides the structure for the Active Directory (AD) JNDI Identity Feeds service. The AD JNDI Identity Feed service is used to feed identity data in the Active Directory server. The parent class is top.

Table 157. erADJNDIFeed table

Attribute name	Description	Type
erServiceName	Name that is on the user interface. This attribute is required.	directory string
erURL	URL of the data source. Supported protocols include: file, http, and https. This attribute is required.	directory string

Table 157. erADJNDIFeed table (continued)

Attribute name	Description	Type
erPassword	Key to authenticate the data source for the JNDI client.	directory string
erUid	Name of the principal to authenticate the data source for the JNDI client.	directory string
Ernamingattribute	The naming attribute on a service used to define the distinguished names of entries in the feed.	directory string
Ernamingcontexts	Identifies the location of identity feed data in the data source. This attribute is required.	distinguished name
erPersonProfileName	Name of the profile to be used for the identity feed.	directory string
erAttrMapFilename	A full path name of a file that contains a mapping of attributes for the identity feed.	directory string
erPlacementRule	A script fragment that defines the location of the user within the organization chart during the HR feed.	binary
erpersonsearchfilter	An LDAP filter to scope which data is to be used for identity feed.	directory string
erUseWorkflow	Indication if the identity feed is to be processed by using the workflow engine.	Boolean
erEvaluateSoD[2]	Indication if the separation of duty policy is to be evaluated when workflow is used for the feed.	Boolean

[1] Indicates the class is added in release 5.0.

[2] Indicates the class is added in release 5.1.

erAttributeConstraint

The erAttributeConstraint class provides the IBM Security Identity Manager structure for an attribute constraint. The parent class is top.

Table 158. erAttributeConstraint table

Attribute name	Description	Type
erOid	Attribute Object Identification Number (Oid). This attribute is required.	directory string
cn	Name of the constraint on the attribute.	directory string
erType	Attribute type.	directory string
erIsReadOnly	True, if this attribute is read-only.	Boolean
erDefaultValue	Attribute default values.	directory string
erCustomConstraint	Attribute definition constraints.	directory string

erChallenges

The erChallenges class provides the structure for administrator-defined questions of password challenge and response. The parent class is top.

Table 159. erChallenges table

Attribute name	Description	Type
cn	Name of the challenge and response entry. This attribute is required.	directory string

Table 159. erChallenges table (continued)

Attribute name	Description	Type
erLastModifiedTime	Last time the challenge and response question list of the user was updated.	directory string
erLostPasswordQuestion	Password challenge and response question list of the user.	directory string

erComplianceIssue

The erComplianceIssue class represents the compliance issue of an account. When an account is noncompliant, a compliance issue might be created for an attribute value. The parent class is top.

Table 160. erComplianceIssue table

Attribute name	Description	Type
erGlobalId	Unique, random ID assigned to all entries in a directory. Used as the regional DN for each entry. This attribute is required.	number string
erAttributeName	Name of account attribute.	directory string
erOverride	Indicates whether the issue is for a non-compliant attribute or disallowed account.	Boolean
erCustomData	Value of the attribute.	directory string
erAttributeAction	Action of the attribute.	integer
erCreateDate	Timestamp (GMT format) of when the object is created.	directory string
erBigCustomData[1]	Large value of the attribute.	binary

[1] Indicates the attribute is added in release 5.0.

erCSVFeed

The erCSVFeed[1] class is a structural class and provides the structure for Identity feed that is in comma-separated value (CSV) format. The parent class is top.

Table 161. erCSVFeed table

Attribute name	Description	Type
erServiceName	Name to display on the user interface. This attribute is required.	directory string
erCSVFileName	A full path name of a CSV file that contains identity data in comma-separated-value format. This attribute is required.	directory string
ernamingattribute	The naming attribute on a service used to define the distinguished names of entries in the feed.	directory string
erPersonProfileName	Name of the profile to be used for the identity feed.	directory string
erPlacementRule	A script fragment that defines the location of the user in the organization chart during the identity feed.	binary

Table 161. erCSVFeed table (continued)

Attribute name	Description	Type
erUseWorkflow	Indication if the identity feed is to be processed by using the workflow engine.	Boolean
erEvaluateSoD[2]	Indication if the separation of duty policy is to be evaluated when workflow is used for the feed.	Boolean

[1] Indicates the class was added in release 5.0.

[2] Indicates the attribute was added in release 5.1.

erDSMLInfoService

Table 162. erDSMLInfoService table

Attribute name	Description	Type
erServiceName	The display name for service instances. This attribute is required.	directory string
erDSMLFileName	The name of a DSML file stored on disk.	directory string
erUseWorkflow	A Boolean flag used on a DSMLInfoService to indicate that people are to be processed by the workflow engine.	Boolean
erUid	An identifier used to uniquely identify a user of a service.	directory string
erPassword	A password used to authenticate a user.	binary
erPlacementRule	A script fragment that defines the location of the user in the organization chart.	binary
erproperties	Defines protocol and behavior properties for service profiles.	directory string
erprotocolmappings	Specifies the service attributes that must be used in messages sent to managed resources.	directory string
erserviceproviderfactory	Defines the name of the Java class for creating the ServiceProvider used to communicate with the managed resource.	directory string
erxforms	Defines transforms for IBM Security Identity Manager adapters.	binary
erEvaluateSoD[1]	Indication if the separation of duty policy is to be evaluated when workflow is used for the feed.	Boolean

[1] Indicates the attribute is added in release 5.1.

erDSML2Service

The erDSML2Service class provides the Directory Service Markup Language Version 2 (DSMLv2) class to import data into IBM Security Identity Manager. The parent class is top.

Table 163. erDSML2Service table

Attribute name	Description	Type
erCategory	Type of entity to manage. This attribute is required.	directory string
erServiceName	Name to display on the user interface. This attribute is required.	directory string
erURL	URL of the data source. Supported protocols include: file, http, and https. This attribute is required.	directory string
erPassword	Key to authenticate DSMLv2 clients for the JNDI client.	binary

Table 163. erDSML2Service table (continued)

Attribute name	Description	Type
erPlacementRule	Placement rule that defines a script to place entries in the organization chart.	binary
erUid	Name of the principal to authenticate DSMLv2 clients for the JNDI client.	directory string
erUseWorkflow	Boolean flag to indicate whether to use workflow to manage data. A value of true evaluates provisioning policies and places an entry in the audit trail.	boolean
ernamingattribute	The naming attribute on a service used to define the distinguished names of entries in event notification.	directory string
Ernamingcontexts[1]	Identifies the service. This attribute is required when Security Identity Manager is acting as a DSMLv2 service.	distinguished name
erEvaluateSoD[2]	Indication if the separation of duty policy is to be evaluated when workflow is used for the feed.	boolean

[1] The namingcontext attribute is deprecated and is replaced with ernamingcontexts in release 5.0.

[2] Indicates the attribute is added in release 5.1.

erGroupItem

The erGroupItem[1] class is an auxiliary class to represent a service group to which the account belongs. The parent class is top.

Table 164. erGroupItem table

Attribute name	Description	Type
erGroupId	Unique identifier of the service group.	directory string
erGroupName	Name of the service group.	directory string
erGroupDescription	Description of the service group.	directory string
erURI[3]	The universal resource identifier.	directory string

[1] Indicates the class was added in release 5.0.

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erHostedAccountItem

The erHostedAccountItem class is an auxiliary class that is added to account entries for hosted services (that is, represented by erHostedService entries). The erHost attribute holds a reference to the owned service entry and provides a more efficient search when it tries to identify the owned service. The parent is erAccountItem.

Table 165. erHostedAccountItem table

Attribute name	Description	Type
erHost	Distinguished name of owned service entry.	distinguished name

erHostedService

The erHostedService class describes a hosted service. The erHostedService class is a domain entry. The parent class is top.

Table 166. erHostedService table

Attribute name	Description	Type
erServiceName	Name of the service. This attribute is required.	directory string
erService	DN of the target service to be managed. This attribute is required.	distinguished name
erObjectProfileName	Service profile name for target service. This attribute is required.	directory string

erHostSelectionPolicy

The erHostSelectionPolicy class provides the structure for a host selection policy. The parent class is erPolicyItemBase.

Table 167. erHostSelectionPolicy table

Attribute name	Description	Type
erJavaScript	Contains a scriptlet used at run time to return a service instance. This attribute is required.	binary
erObjectProfileName	Name corresponding to the service type. This attribute is required.	directory string
erUserClass	Name of a user class, such as Person or BPPerson. This attribute is required.	directory string

erITIMService

The erITIMService class provides the IBM Security Identity Manager structure for Security Identity Manager service. The parent class is top.

Table 168. erITIMService table

Attribute name	Description	Type
erServiceName	Security Identity Manager service name. This attribute is required.	directory string
owner	Service owner (person).	distinguished name
erRepositoryService[3]	The existing account repository used by Security Identity Manager for authentication.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erJNDIFeed

The erJNDIFeed[1] class is a structural class and provides the structure for InetOrgPerson JNDI Identity Feeds service. The parent class is top.

Table 169. erJNDIFeed table

Attribute name	Description	Type
erServiceName	Name to display on the user interface. This attribute is required.	directory string
erURL	URL of the data source. Supported protocols include: file, http, and https. This attribute is required.	directory string

Table 169. erJNDIFeed table (continued)

Attribute name	Description	Type
erPassword	Key to authenticate the data source for the JNDI client.	directory string
erUid	Name of the principal to authenticate the data source for the JNDI client.	directory string
ernamingattribute	The naming attribute on a service used to define the distinguished names of entries in the feed.	directory string
ernamingcontexts	Identifies the location of identity feed data in the data source. This attribute is required.	distinguished name
erPersonProfileName	Name of the profile to be used for the identity feed.	directory string
erAttrMapFilename	A full path name of a file that contains a mapping of attributes for the identity feed.	directory string
erPlacementRule	A script fragment that defines the location of the user in the organization chart during the HR feed.	binary
erpersonsearchfilter	An LDAP filter to scope which data is to be used for identity feed.	directory string
erUseWorkflow	Indication if the identity feed is to be processed by using the workflow engine.	Boolean

[1] Indicates the class was added in release 5.0.

erJoinDirective

The erJoinDirective class provides the structure for a join directive used in merging provisioning parameters. The parent class is top.

Table 170. erJoinDirective table

Attribute name	Description	Type
erAttributeName	Name of service attribute. This attribute is required.	directory string
erDirectiveType	Type of join directive to be used. This attribute is required.	directory string
description	Description of how the directive is used.	directory string
erCustomData	Contains any parameters to be passed to the class that implements the JoinDirective interface.	directory string
erPrecedenceSequence	Sequence of allowed values for a single valued attribute with the most preferable values listed first.	directory string

erPrivilegeRule

The erPrivilegeRule class provides the structure for a privilege rule used in privileges of account attributes. The parent class is top.

Table 171. erPrivilegeRule table

Attribute name	Description	Type
erAttributeName	Name of account attribute. This attribute is required.	directory string

Table 171. erPrivilegeRule table (continued)

Attribute name	Description	Type
erDirectiveType	Type of join directive to be used. This attribute is required. Possible values: 0 – Never generate alert 1 – Always generate alert 2 – Numeric order (higher value generates alert) 3 – Numeric order (lower value generates alert) 4 – Precedence sequence	directory string
erPrecedenceSequence	Sequence of allowed values for a single valued attribute with the most preferable values listed first.	directory string

erObjectCategory

The erObjectCategory class provides the structure for an entity type. The parent class is top.

Table 172. erObjectCategory table

Attribute name	Description	Type
erType	Name of the entity category. This attribute is required.	directory string
erXML	Object Operation definition for lifecycle management.	binary
erLifecycleRule	LifecycleRule data structure for lifecycle management.	binary

erObjectProfile

The erObjectProfile class provides the IBM Security Identity Manager structure for an object profile. The parent class is top.

Table 173. erObjectProfile table

Attribute name	Description	Type
erObjectProfileName	Profile name. This attribute is required.	directory string
erCategory	Entity category such as Person, Role, System User, or other category.	directory string
erCustomClass	Name of the class used to create an entity.	directory string
erRdnAttr	Name attribute.	directory string
erSearchAttr	Search attribute.	directory string
erAttrMap	Map of the logical attribute name and physical attribute name. Key: logical attribute name.	directory string
erXML	ObjectOperation data structure for lifecycle management.	binary
erLifecycleRule	LifecycleRule data structure for lifecycle management.	binary
description[1]	Description of the profile.	directory string
erCustomProperties[2]	List of properties that are defined on the profile. Key = property value. For example, Managed=true.	directory string
erDaoClass[3]	The data access object implementation class name.	directory string

[1] Indicates the attribute is added in release 5.0.

[2] Indicates the attribute is added in release 5.1.

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erLifecycleProfile

The erLifecycleProfile class provides the IBM Security Identity Manager structure for a lifecycle profile on an entity. The parent class is top.

Table 174. erLifecycleProfile table

Attribute name	Description	Type
erGlobalId	Unique, random ID assigned to all entries in a directory. Used as the regional DN for each entry. This attribute is required.	number string
erEntityTarget	Distinguished name of the entity that the lifecycle profile is defined for. This attribute is required.	distinguished name
cn	Name of the object.	directory string
erXML	ObjectOperation data structure for lifecycle management.	binary

erRemoteServiceItem

The erRemoteServiceItem class is an auxiliary class that describes a hosted service. The parent class is erServiceItem.

Table 175. erRemoteServiceItem table

Attribute name	Description	Type
erUid	The login ID of the user for the service.	directory string
erPassword	The password of the user.	binary
erCheckPolicy	Flag to determine whether to check the user against the defined policies.	Boolean
erDisallowedAction	The action to be taken during reconciliation if an account is prevented by a provisioning policy. Possible values are: Log Only Suspend Delete	directory string
erConstraintViolationAction	The action to be taken during reconciliation if an account is prevented by a provisioning policy but the account values are not compliant. Possible values are: Log Only Overwrite Local Values Overwrite Remote Values	directory string
erIdentityLookupMethod	The method used during reconciliation to look up the identity of the account owner. The only possible value is Alias.	directory string

erServiceItem

The erServiceItem class is an auxiliary class that describes an owned service. This class is a domain entry. The parent class is top.

Table 176. erServiceItem table

Attribute name	Description	Type
erServiceName	Name of the service.	directory string

Table 176. erServiceItem table (continued)

Attribute name	Description	Type
owner	DN of the service owner.	distinguished name
erPrerequisite	Required prerequisite for the account.	distinguished name
erNonComplianceAction	Compliant action for accounts of the service. Possible values are: • Mark NonCompliant (0) • Suspend NonCompliant (1) • Correct NonCompliant (2) • Use Workflow (3) • Use Global Settings (4)	integer
erAlertOption	Option settings for when compliance alert is triggered. Only applicable when compliant action is set to 3 (Use Workflow). Possible values are: • Reconciliation (0) • Policy change (1) • Person data change (2) • Account data change (3)	integer
description	Description of the service.	directory string
erConnectionMode[3]	The current Connection Mode of the Service Instance, such as Manual or Automatic.	directory string
erURI[3]	The universal resource identifier.	directory string
erTag[3]	The service tag.	directory string
erServiceSSOMapping[3]	Corresponding IBM Security Access Manager ESSO Service ID for a service item.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erServiceProfile

The erServiceProfile class provides the IBM Security Identity Manager structure for a service profile. The parent class is erObjectProfile.

Table 177. erServiceProfile table

Attribute name	Description	Type
erAccountClass	Name of a custom class used to create an account.	directory string
erAccountName	Name of profile associated with the account.	directory string
erproperties	Service attributes used in messages sent to the managed resources. This attribute is required.	directory string
erprotocolmappings	Service attributes used in messages sent to the managed resources.	directory string
erserviceproviderfactory	Name of the Java class to create the ServiceProvider used to communicate with the managed resource. This attribute is required.	directory string
erxforms	Defines transforms for Security Identity Manager adapters.	binary
erserivcesupportclass	List of objectclass that is used for services that support data, such as group.	directory string
ergroupmappings[1]	A map of account attribute for a group.	directory string
erOpRequired[1]	List of required attributes per service or account operation.	directory string (1000)
erOpSend[1]	List of send-only attributes per operation.	directory string (1000)
erOpMultiReplace[1]	List of replace-multi-value attributes per operation.	directory string (1000)
erOpSingleAddDelete[1]	List of add-delete-single-value attributes per operation.	directory string (1000)
erAttributeHandler[1]	Name of the attribute handler class.	directory string (1000)
erComplexAttributes[1]	Name of the complex attribute list.	directory string (1000)

[1] Indicates the attribute was added in release 5.0.

erSystemItem

The erSystemItem class provides the IBM Security Identity Manager auxiliary class for the Security Identity Manager system. The parent class is top.

erSystemRole

The erSystemRole class represents a system role, however, it does not include membership information. Members are defined in erSystemUser.erRoles. This class is a domain entry. The parent class is top.

Table 178. erSystemRole table

Attribute name	Description	Type
erRoleName	The system role name. This attribute is required.	directory string
description	Description of the role.	directory string
erSystemRoleCategory	Level of access – End User, Supervisor, System Administrator.	integer
erURI[3]	The universal resource identifier.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erSystemUser

The erSystemUser class stores IBM Security Identity Manager system accounts such as the pre-defined Security Identity Manager system account. The erAccountItem is also added to each erSystemUser entry since it is an account managed by the system. This class is a domain entry. The parent class is top.

Table 179. erServiceProfile table

Attribute name	Description	Type
erUid	Account login ID. This attribute is required.	directory string
erLostPasswordQuestion	Account lost password question.	directory string
erLostPasswordAnswer	Account lost password answer.	binary
erIsDelegated	Flag determining whether the account workflow can be sent to delegates.	Boolean
erDelegate	Delegate of the user.	directory string
erWorkflow	Filter for viewing pending requests and completed requests.	directory string
erRoles	Roles associated with the account.	distinguished name
erHomePage	Login home page.	directory string
erPswdLastChanged	Date and time that the password was last changed.	generalized time
erNumLogonAttempt	Number of times that the user attempted to log on.	integer
erChangePswdRequired	Flag indicating whether the user is required to change the password the next time that the user logs on to the system.	Boolean
erRespLastChange	Date and time that the challenge response was last changed.	generalized time

Policy classes

There are several types of policies: password, identity, provisioning, adoption, recertification, separation of duty, and account defaults. These policies all share some general attributes. These attributes are represented in the erPolicyBase and erPolicyItemBase classes. The erPolicyBase class inherits from the erPolicyItemBase class. All policies are domain entries.

erAccountTemplate

The erAccountTemplate[1] class stores account default-specific attributes. The parent class is erPolicyBase.

Table 180. erAccountTemplate table

Attribute name	Description	Type
erStaticDefaultAttrMap	Static default (attribute=value) pair for account defaults.	binary
erScriptedDefaultAttrMap	Scripted default (attribute=value) pair for account defaults.	binary

[1] Indicates the class is added in release 5.0.

erAdoptionPolicy

The erAdoptionPolicy class stores adoption policy-specific attributes. The parent class is erPolicyBase.

Table 181. erAdoptionPolicy table

Attribute name	Description	Type
erJavaScript	Script that resolves the owner for an adoption account.	binary

erIdentityPolicy

The erIdentityPolicy class stores identity policy-specific attributes. The parent class is erPolicyBase.

Table 182. erIdentityPolicy table

Attribute name	Description	Type
erJavaScript	Script that is evaluated to create the user ID.	binary
erUserClass	Class home of the user.	directory string

erPasswordPolicy

The erPasswordPolicy class stores password policy-specific attributes. The parent class is erPolicyBase.

Table 183. erPasswordPolicy table

Attribute name	Description	Type
erXML	XML document containing password rules. This attribute is required.	binary

erPolicyBase

The erPolicyBase class stores commonly used functional attributes such as state information and the target of the policy. The parent class is erPolicyItemBase.

Table 184. erPolicyBase table

Attribute name	Description	Type
erPolicyTarget	Services or service instances targeted by the policy. If a service instance is targeted, the value is the string that represents the service instance DN. **Format:** 1;<*value*> If a service profile is targeted, the value is the name of the service profile. **Format:** 0;<*value*> If all services are targeted, the value is *. **Format:** 2;<*> If a service selection policy is targeted, the value is the name of the service profile affected by the service selection policy. **Format:** 3;<*value*>	directory string
erReqPolicyTarget	Lists required policy targets (service instance or service profile).	directory string

erPolicyItemBase

The erPolicyItemBase class stores general bookkeeping attributes for policies, such as name and description. The parent class is top.

Table 185. erPolicyItemBase table

Attribute name	Description	Type
erPolicyItemName	The policy name. This attribute is required.	directory string
erLabel	The label name for the policy.	directory string
erKeywords	A list of key words.	directory string
description	A description of the policy.	directory string
erEnabled	Flag indicating whether the policy participates in the provisioning process. If the flag is enabled, the policy participates in the provisioning process. If the flag is disabled, the policy does not participate in the provisioning process.	Boolean
erScope	Determines which service instances are governed by this policy. Single-level scope limits the policy to affect only those service instances at the same level as the policy. With subtree scope, a policy affects service instances at the same level as the policy and service instances in levels below the policy.	integer
erURI[3]	The universal resource identifier.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erProvisioningPolicy

The erProvisioningPolicy class stores provisioning policy-specific attributes. The parent class is erPolicyBase.

Table 186. erProvisioningPolicy table

Attribute name	Description	Type
erEntitlements	Policy access definitions. This attribute is required.	binary
erPriority	The priority level for this policy. This attribute is required.	integer
erPolicyMembership	Policy principals. Identifies users who are governed by this policy. This attribute is required.	directory string
erDraft	True if the policy is saved as draft.	Boolean
erOriginalPolicyDN	Distinguished name of original policy.	distinguished name

Table 186. erProvisioningPolicy table (continued)

Attribute name	Description	Type
erEntitlementOwnershipTypes[3]	The entitlement ownership types.	directory string

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

erRecertificationPolicy

The erRecertificationPolicy[1] class stores recertification policy-specific attributes. The parent class is erPolicyBase.

Table 187. erRecertificationPolicy table

Attribute name	Description	Type
erType	Type of entities this recertification policy governs. Values include: ACCOUNT – for account entities ACCESS – for access entities IDENTITY – for user entities[2]	directory string
erIsCustom	Indication whether this recertification policy is customized (true/false).	Boolean
erRecertifier	Information of the participant who receives the recertification notice or work item.	directory string
erSchedulingMode	The recertification schedule mode. Values: CALENDAR ROLLING The CALENDAR mode is only for access recertification.	directory string
erRollingInterval	The recertification period (in days) if erSchedulingMode is ROLLING. Will not have a value if erSchedulingMode is not ROLLING.	integer
erTimeoutAction	The action to take upon recertification timeout. Values: APPROVE REJECT NONE 2	directory string
erTimeoutPeriod	The timeout period for recertification process (in days).	integer
erRejectAction	The action to take on the account/access when recertification is rejected. Values: MARK SUSPEND DELETE	directory string
erRejectNotify	Information of the participant who receives the rejection notice upon rejection of the recertification notice or work item.	directory string
erRecertTemplateDN	DN pointing to the notification template used for the initial recertification notice.	distinguished name

Table 187. erRecertificationPolicy table (continued)

Attribute name	Description	Type
erRecertRejectTemplateDN	DN pointing to the notification template used for the rejection notice.	distinguished name
erUserClass	The person category for the recertification policy. Values: ALL PERSON BPPERSON	directory string
erSchedule	Information of the schedule for the recertification policy.	directory string
erLifecycleRule	The lifecycle rule information for the policy.	binary
erXML	XML content of the workflow operations for the policy.	binary
erGlobalID	Unique ID of the policy.	number string
erLifecycleEnable	Indication whether the policy has a lifecycle operation defined. Values: True False. Always true for recertification policy.	Boolean

[1] Indicates the class was added in release 5.0.

[2] Indicates the attribute value was added in release 5.1.

erSeparationOfDutyPolicy

The erSeparationOfDutyPolicy[1] class stores separation of duty policy-specific attributes. The parent class is erPolicyBase.

Table 188. erSeparationOfDutyPolicy table

Attribute name	Description	Type
Owner	Multivalue attribute pointing to the owner of this policy. Can be any combination of DNs pointing to persons or roles.	distinguished name
erXML	Unused attribute reserved for future use.	binary

[1] Indicates the class was added in release 5.1.

erSeparationOfDutyRule

The erSeparationOfDutyRule[1] class stores separation of duty policy rule-specific attributes. The parent class is top.

Table 189. erSeparationOfDutyPolicy table

Attribute name	Description	Type
cn	Name of the separation of duty policy rule (required).	directory string
erCardinality	Number of roles allowed.	
erRoles	Multivalue attribute pointing to the DNs of the roles that are involved in this separation of duty policy rule. This attribute is the expanded hierarchy of roles that relate to the erAffectedRoles attribute of this entry.	distinguished name
erAffectedRoles	Multivalue attribute pointing to the DNs of the roles that are explicitly defined in this separation of duty policy rule.	distinguished name
erURI[3]	The universal resource identifier.	directory string

[1] Indicates the class was added in release 5.1.

[3] Indicates the attribute is added in IBM Security Identity Manager 6.0.

Chapter 3. Auditing schema tables

The audit event schema has a common base event table, `audit_event`, which contains fields common to all audit events.

Separate tables are created for an event type only if that event type contains attributes, which are not generic enough to keep in a common table. As a rule, any element that is common to most audit events is kept in the `audit_event` container table. This design choice helps reduce the number of table joins when event data is queried.

The auditing event information is in the following tables:

Table 190. Auditing schema tables

Event Category	**Table Name**
Common tables	`AUDIT_EVENT`
Authentication	No event-specific table
Person management	`AUDIT_MGMT_TARGET` This table is used only if action=Person transfer.
Delegate authority	`AUDIT_MGMT_DELEGATE`
Policy management	No event-specific table
ACI management	No event-specific table

"Access request management" on page 125	`AUDIT_MGMT_ACCESS_REQUEST`
	
	`AUDIT_MGMT_OBLIGATION`
	
	`AUDIT_MGMT_OBLIGATION_ATTRIB`
	
	`AUDIT_MGMT_OBLIGATION_RESOURCE`
	
	`AUDIT_MGMT_MESSAGE`

"Manual activity events" on page 130	`AUDIT_MGMT_ACTIVITY`
	
	`AUDIT_MGMT_PARTICIPANT`

"Lifecycle rule events" on page 138	No event-specific table
Account management	`AUDIT_MGMT_PROVISIONING`
Container management	No event-specific table
Organization role management	`AUDIT_MGMT_TARGET` This table is used only if action=Add Member or Remove Member.
ITIM group management	`AUDIT_MGMT_TARGET` This table is used only if action=Add Member or Remove Member.
Service management	`AUDIT_MGMT_TARGET` This table is used only if Action=Add, Modify, or Remove Adoption Rule.
Group management	No event-specific table

Table 190. Auditing schema tables (continued)

Event Category	Table Name
Service policy enforcement	No event-specific table
Reconciliation	No event-specific table
Entitlement workflow management	No event-specific table
Entity operation management	No event-specific table
System configuration	No event-specific table
Runtime events	No event-specific table
Self-password change	No event-specific table
"Migration" on page 158	No event-specific table
Credential management	No event-specific table
Credential Pool management	No event-specific table
Credential Lease management	AUDIT_MGMT_LEASE This table is used only if the action is Checkout or if the credential is a pool member.

AUDIT_EVENT table

The AUDIT_EVENT table is common for all audit events. However, the value for some columns is different depending on the event. See the specific event for the column values.

Table 191. AUDIT_EVENT table

Column Name	Column Description	Data type
ID*	ID by which this event is identified. Primary key.	Numeric
ITIM_EVENT_CATEGORY*	Security Identity Manager type of the event	Character (50)
ENTITY_NAME	Name of the Security Identity Manager entities altered by this event. The size of this column is 100 characters, which assumes that the name of the entity that is being audited is 100 or less character long.	Character (1000)
ENTITY_DN	DN of the entity involved in this event.	Character (1000)
ENTITY_TYPE	Type of the Security Identity Manager entity.	Character (50)
ACTION*	The value of this column depends on the event type. Each event type has a set of actions.	Character (25)
WORKFLOW_PROCESS_ID	Process ID of the workflow initiated. This column is applicable to workflow operations.	Numeric
INITIATOR_NAME	The user ID of the ITIM account that submitted the request.	Character (1000)
INITIATOR_DN	The distinguished name of the ITIM account that submitted the request.	Character (1000)
INITIATOR_TYPE	PERSON - Indicates that the request was submitted by a person. SYSTEM - Indicates that the request was submitted by the Security Identity Manager system.	Character (50)
INITIATOR_PERSON_DN	Distinguished name of the person who submitted the request.	Character (1000)
INITIATOR_PERSON_NAME	Name of the person who submitted the request.	Character (1000)

Table 191. AUDIT_EVENT table (continued)

Column Name	Column Description	Data type
CONTAINER_NAME	Name of the container that holds the entity.	Character (1000)
CONTAINER_DN	Distinguished name of the container that holds the entity.	Character (1000)
RESULT_SUMMARY	The results of an event: Success Failure If the operation is submitted to workflow, this column indicates whether the operation was successfully submitted to workflow.	Character (25)
TIMESTAMP*	The time when the audit event occurs. It is also a start time of the operation.	Character (50)
COMMENTS	Description for this event.	Character (1000)
TIMESTAMP2	The time stamp for when the event was completed.	Character (50)

* Indicates the column is required and not null.

IBM Security Identity Manager authentication

This section describes the columns used by events related to Security Identity Manager authentication operations.

Values for columns in the AUDIT_EVENT table

The following table describes the values of columns used by authentication operations in the AUDIT_EVENT table.

Table 192. Column values in the AUDIT_EVENT table

Column Name	Values
ITIM_EVENT_CATEGORY	IBM Security Identity Manager Authentication
ENTITY_TYPE	Entity type: ChallengeResponse BasicAuth
ACTION	Authentication getAuthenticatedObject

Table columns in the AUDIT_EVENT table

The following list shows the columns for each IBM Security Identity Manager authentication action in the AUDIT_EVENT table.

Autheticate

```
entity_name, entity_type, result_summary, initiator_name,
initiator_dn, timestamp
```

getAuthenticatedObject

```
entity_name, entity_type, result_summary, initiator_name,
initiator_dn, timestamp
```

Person management

This section describes the columns used by events related to Person management, such as add, modify, delete, suspend, transfer, and restore.

In addition to the AUDIT_EVENT table, these tables are used by person management events: AUDIT_MGMT_TARGET, AUDIT_MGMT_ACCESS_REQUEST, AUDIT_MGMT_OBLIGATION, AUDIT_MGMT_OBLIGATION_ATTRIB, and AUDIT_MGMT_OBLIGATION_RESOURCE.

AUDIT_MGMT_TARGET table

The AUDIT_MGMT_TARGET table is used if the action is Transfer.

Table 193. AUDIT_MGMT_TARGET table

Column Name	Column Description	Data type
EVENT_ID*	Identification that is assigned to the event. References AUDIT_EVENT (ID).	Numeric
TARGET_ENTITY_NAME	The name of container to which the person is being transferred. Applicable if action=Transfer	Character (1000)
TARGET_ENTITY_DN	The DN of container to which the person is being transferred. Applicable if action=Transfer	Character (1000)
TARGET_ENTITY_TYPE	The type of container to which the person is being transferred.	Character (50)

* Indicates the column is required and not null.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the person management events in the AUDIT_EVENT table.

Table 194. Values for columns in the AUDIT_EVENT table

Column Name	Value
ITIM_EVENT_CATEGORY	Person Management.
ENTITY_NAME	Name of the person.
ENTITY_DN	Distinguished name of the person.
ENTITY_TYPE	Type of person, such as person, business person, or custom person.
INITIATOR_NAME	The user ID of the ITIM account that submitted the request.
INITIATOR_DN	The distinguished name of the ITIM account that submitted the request.
INITIATOR_TYPE	PERSON - Indicates that the request was submitted by a person. SYSTEM - Indicates that the request was submitted by the Security Identity Manager system.
INITIATOR_PERSON_DN	Distinguished name of the person who submitted the request.
INITIATOR_PERSON_NAME	Name of the person who submitted the request.
CONTAINER_NAME	Name of the container that holds the entity.
CONTAINER_DN	Distinguished name of the container that holds the entity.
WORKFLOW_PROCESS_ID	Process ID of the initiated workflow.

Table 194. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
RESULT_SUMMARY	Result of operation: Submitted – submitted to workflow successfully
ACTION	Types of actions: Add – add a person Modify – modify a person Delete – delete a person Suspend – suspend a person Restore – restore a person Transfer – transfer a person

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management event in the AUDIT_EVENT table.

Add Person event

```
entity_name, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

Delete Person event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

Modify Person event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

Restore Person event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

Suspend Person event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

Transfer Person event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
,workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

From **AUDIT_MGMT_TARGET** table: target_entity_name, target_entity_dn

Self-Register event

entity_name, entity_type, workflow_process_id, container_name, container_dn, timestamp, result_summary

Table columns for person management in the AUDIT_MGMT_ACCESS_REQUEST table

The following list shows the columns for all person management event in the AUDIT_MGMT_ACCESS_REQUEST table.

- Event_ID
- Wokflow_Process_Id
- Action
- Access_Obligations_Ids
- Status
- Completed_Date
- Person_Name
- Person_DN

Table columns for person management in the AUDIT_MGMT_OBLIGATION table

The following list shows the columns for all person management event in the AUDIT_MGMT_OBLIGATION table.

- Event_ID
- Id
- Obligation_Type
- System_Generated

AUDIT_MGMT_OBLIGATION_ATTRIB table

The **AUDIT_MGMT_OBLIGATION_ATTRIB** table contains information about attributes of the obligations. These obligations are related to Access Management, Person Management, and Account Management that are submitted through the administrative console, Self-service user interface, and the Identity Service Center user interface.

The **AUDIT_MGMT_OBLIGATION_ATTRIB** table contains the following columns.

Table 195. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_ATTRIB** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
OBLIGATION_ID*	Identifier of the obligation to which the resources are related.	Numeric
ATTRIBUTE_NAME*	Name of an attribute that is associated to the obligation.	Character (225)
ATTRIBUTE_VALUE*	Data value of an attribute that is associated to the obligation.	Character (4000)
ATTRIBUTE_PREVIOUS_VALUE	Previously stored data value of an attribute that is associated to the obligation before an edit action.	Character (4000)

Table 195. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_ATTRIB** *table (continued)*

Column name	Column description	Data type
SEQUENCE_NO*	A generated numerical value that starts at 1 and increments by 1. It enables the persistence of an attribute name with multiple attribute values.	SMALLINT

* Indicates the column is required and not null.

AUDIT_MGMT_OBLIGATION_RESOURCE table

The **AUDIT_MGMT_OBLIGATION_RESOURCE** table contains information about the obligation resource attributes.

The **AUDIT_MGMT_OBLIGATION_RESOURCE** table contains the following columns.

Table 196. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_RESOURCE** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
OBLIGATION_ID*	Identifier of the obligation to which the resources are related.	Numeric
RESOURCE_TYPE*	The value can be **ACCOUNT**, **PERSON**.	Character (50)
RESOURCE_NAME*	Name of the resource to which access is requested.	Character (1000)
RESOURCE_DN*	Distinguished name of the resource to which access is requested.	Character (1000)

* Indicates the column is required and not null.

Delegate authority

This section describes events related to delegate authority, such as add and modify.

AUDIT_MGMT_DELEGATE table

The AUDIT_MGMT_DELEGATE table is used if the action is to delegate a member.

Table 197. *AUDIT_MGMT_DELEGATE table*

Column Name	Column Description	Data type
EVENT_ID*	ID by which this event is identified. References AUDIT_EVENT (ID).	Numeric
DELEGATE_NAME	The name of the account to which authorities are delegated.	Character (1000)
DELEGATE_DN	The DN of the account to which authorities are delegated.	Character (1000)
DELEGATE_START_TIME	Start time of the delegation.	Character (1000)
DELEGATE_END_TIME	End time of the delegation.	Character (1000)

* Indicates the column is required and not null.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the Person management operations in the AUDIT_EVENT table.

Table 198. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Delegate authority.
entity_name	Name of the account whose rights are being delegated.
entity_dn	Distinguished name of the account whose rights are being delegated.
entity_type	Account.
workflow_process_id	Process ID of the initiated workflow.
result_summary	Result of operation: Submitted – submitted to workflow successfully
Action	Types of actions: Add – Delegate authority Modify – Modify a delegate

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management action in the AUDIT_EVENT table.

- **Add Delegate event**

  entity_name, entity_dn, initiator_name, initiator_dn, timestamp, result_summary

  From Audit_Delegate table:

  delegate_name, delegate_dn, delegate_starttime, delegate_endtime

- **Modify Delegate event**

  entity_name, entity_dn, initiator_name, initiator_dn, timestamp, result_summary

  From Audit_Delegate table:

  delegate_name, delegate_dn, delegate_starttime, delegate_endtime

Policy management

This section describes events related to IBM Security Identity Manager polices, such as provisioning, service selection, identity, password, separation of duty, and recertification policies.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the policy management events in the AUDIT_EVENT table.

Table 199. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Policy Management.
entity_name	Name of the policy.
entity_dn	Distinguished name of the policy.

Table 199. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
entity_type	Types of policy entities: ProvisioningPolicy – used to associate one or multiple groups of users with one or multiple entitlements. The group of users is typically identified by organization or organization role. The entitlement is a construct to define a set of permissions, or privileges, on a managed provisioning resource. HostSelectionPolicy – (service selection policy) used in situations where there is an iinstance of a provisioning resource on which the provisioning of an account is to take place. It is determined dynamically based on account owners attributes. IdentityPolicy – Identity policy specifies how identities, or user IDs, are generated when provisioning one or more resources. PasswordPolicy – A password policy specifies a set of rules that all passwords for one or more services must conform. AccountTemplate – An account template. SeparationOfDutyPolicy – A separation of duty policy. RecertificationPolicy – A recertification policy.
Action	Types of actions: Add – Add a policy Modify – Modify a policy Delete – Delete a policy Reconcile – Separation of duty policy only (evaluation of a separation of duty policy) Exempt – Separation of duty policy only (exempt an existing violation) Revoke – Separation of duty policy only (revoke an approved exemption) SaveAsDraft – Provisioning policy only CommitDraft - Provisioning policy only EnforceEntirePolicy – Provisioning policy only EnforcePolicyImport – Import a policy

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each policy management event in the AUDIT_EVENT table.

Add Host Selection Policy event

```
entity_name, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

Modify Host Selection Policy event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
initiator_type, initiator_person_dn, initiator_person_name,
workflow_process_id, container_name, container_dn, timestamp,
result_summary
```

Delete Host Selection Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Add Provisioning Policy event

entity_name, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Modify Provisioning Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Delete Provisioning Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Enforce Entire Provisioning Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Save Draft Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Commit Draft Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Delete Draft Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Add Identity Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Modify Identity Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Delete Identity Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Add Password Policy event

entity_name, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Modify Password Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp,result_summary

Delete Password Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Add Separation of Duty Policy event

entity_name, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Modify Separation of Duty Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Delete Separation of Duty Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Evaluate Separation of Duty Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Exempt a Violation for a Separation of Duty Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary, comments

Revoke an Exemption for a Separation of Duty Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary, comments

Add Recertification Policy event

entity_name, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Modify Recertification Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn,

initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Delete Recertification Policy event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, container_name, container_dn, timestamp, result_summary

Enforce Policy Import event

itim_event_category, action, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, result_summary

ACI management

This section describes the columns used by events related to IBM Security Identity Manager access control information (ACI).

In addition to the AUDIT_EVENT table, the AUDIT_MGNT_TARGET table is used by ACI management events.

AUDIT_MGMT_TARGET table

The AUDIT_MGMT_TARGET table is used if the action is Add Member or Remove.

Table 200. AUDIT_MGMT_TARGET table

Column Name	Column Description	Value Type	Required?
event_id	ID by which this event is identified. This column contains the foreign key to the ID column of the audit_event table.	long	Yes
target_entity_name	Name of the target ACI for Action = AddAuthOwneror Action=DeleteAuthOwner.	string	Yes for action = AddAuthOwner or Action=DeleteAuthOwner

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the policy management operations in the AUDIT_EVENT table.

Table 201. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	ACI Management.
entity_name	Name of the ACI.
entity_dn	Distinguished name of the ACI.
entity_type	Types of policy entities: aci – Access control list

Table 201. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
action	Types of actions: Add – Add the ACI Modify – Modify the ACI Delete – Delete the ACI AddAuthorizationOwner – Add an authorization owner DeleteAuthorizationOwner – Delete an authorization owner

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each Person management action in the AUDIT_EVENT table.

- **Add ACI event**

  entity_name, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary
- **Modify ACI event**

  entity_name, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary
- **Delete ACI event**

  entity_name, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary
- **Add Authorization Owner event**

  entity_name, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_target: target_entity_name
- **Delete Authorization Owner event**

  entity_name, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_target: target_entity_name

Access request management

Access request management describes the audit data that supports the viewing of access requests that are submitted through the Administrative console, Self-service user interface, and Identity Service Center user interface.

In addition to the AUDIT_EVENT table, access request management events use the following tables.

- AUDIT_MGMT_ACCESS_REQUEST
- AUDIT_MGMT_OBLIGATION
- AUDIT_MGMT_OBLIGATION_ATTRIB
- AUDIT_MGMT_OBLIGATION_RESOURCE
- AUDIT_MGMT_MESSAGE

AUDIT_MGMT_ACCESS_REQUEST table

The **AUDIT_MGMT_ACCESS_REQUEST** table contains information about account, group, person, and role provisioning that is submitted through the Administrative console, Self-service user interface, and Identity Service Center user interface.

The **AUDIT_MGMT_ACCESS_REQUEST** table includes extra audit data that is related to rows in the **AUDIT_EVENT** table for which the **ITIM_EVENT_CATEGORY** column contains these values: **PersonManagement**, **AccountManagement**, **AccessManagement**, **OrgRoleManagement**, and **AccessRequest**.

Table 202. **AUDIT_MGMT_ACCESS_REQUEST** *table for access request management*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**.	Numeric
WORKFLOW_PROCESS_ID*	Identifier of the workflow process to which this additional audit data is related.	Numeric
ACTION*	The supported actions are ADD, MODIFY, CHANGE, DELETE, SUSPEND, RESTORE, TRANSFER, CHANGE_PASSWORD, ADDMEMBER, REMOVEMEMBER, and SELF_REGISTER.	Character (25)
PERSON_NAME **	Name of the person for whom the access request was submitted.	Character (1000)
PERSON_DN **	Distinguished name of the person for whom the access request was submitted.	Character (1000)
ACCESS_CATALOG_ID **	Access catalog identifier of the service, group, or role for which the access request was submitted.	Numeric
ACCESS_CATALOG_NAME**	Access catalog name of the service, group, or role for which the access request was submitted.	Character (1000)
ACCESS_CATALOG_DESCRIPTION**	Access catalog description of the service, group, or role for which the access request was submitted.	Character (1000)
ACCESS_CATALOG_CATEGORY**	Access catalog description of the service, group, or role for which the access request was submitted.	Character (1000)
ACCESS_CATALOG_ICON **	URL of the access catalog icon of the service, group, or role for which the access request was submitted.	Character (1000)
ACCESS_CATALOG_BADGE_1 **	First access catalog badge of the service, group, or role for which the access request was submitted.	Character (3000)
ACCESS_CATALOG_BADGE_2 **	Second access catalog badge of the service, group, or role for which the access request was submitted.	Character (3000)
ACCESS_CATALOG_BADGE_3 **	Third access catalog badge of the service, group, or role for which the access request was submitted.	Character (3000)
ACCESS_CATALOG_BADGE_4 **	Fourth access catalog badge of the service, group, or role for which the access request was submitted.	Character (3000)

Table 202. **AUDIT_MGMT_ACCESS_REQUEST** *table for access request management (continued)*

Column name	Column description	Data type
ACCESS_CATALOG_BADGE_5 **	Fifth access catalog badge of the service, group, or role for which the access request was submitted.	Character (3000)
ACCESS_OBLIGATION_IDS*	List of obligation IDs separated by semicolons that identifies the obligations that must be fulfilled for the access request.	Character (4000)
SERVICE_NAME	Name of the service for which the account or access request was submitted.	Character (1000)
STATUS*	Status of the access request. The **STATUS** contains one of the following values. FULFILLED NOT_FULFILLED PENDING	Character (25)
COMPLETED_DATE*	Date and time when the access request is completed or canceled.	Character (50)

* Indicates the column is required and not null.

** Indicates the column is null if the event category is not **AccessRequest**.

Note: The **AUDIT_MGMT_ACCESS_REQUEST** table contains multiple rows that have the same **WORKFLOW_PROCESS_ID** column value if there is more than one access that is associated with the corresponding request.

AUDIT_MGMT_OBLIGATION table

The **AUDIT_MGMT_OBLIGATION** table contains information about obligations. These obligations are related to Access Management, Person Management, and Account Management that are submitted through the administrative console, Self-service user interface, and the Identity Service Center user interface.

The **AUDIT_MGMT_OBLIGATION** table contains the following columns.

Table 203. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
ID*	Identifier of the activity. The value of this column serves as a foreign key for the **AUDIT_MGMT_OBLIGATION_ATTRIB** and **AUDIT_MGMT_OBLIGATION_RESOURCE** tables.	Numeric
PERSON_DN*	Distinguished name of the person for whom the access request was submitted to which the obligation is related.	Character (1000)

Table 203. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION** *table (continued)*

Column name	Column description	Data type
OBLIGATION_TYPE*	Type of the obligation. CREATE_ACCOUNT, MODIFY_ACCOUNT, DELETE_ACCOUNT, SUSPEND_ACCOUNT, and RESTORE_ACCOUNT SET_SYNCPASSWORD, SELECT_ACCOUNTS, and CHANGE_PASSWORD CREATE_PERSON, MODIFY_PERSON, DELETE_PERSON, SUSPEND_PERSON, RESTORE_PERSON, TRANSFER_PERSON, and SELF_REGISTER.	Character (50)
SYSTEM_GENERATED*	Indicates whether the obligation was system-generated. Values are Y or N	Character (1)
ACCESS_FORM_TEMPLATE	Form template in JSON format that presents related attributes in the **CREATE_ACCOUNT** obligation. Form template is shown only if the create account request is submitted from Identity Service Center.	Long character (100 K)

* Indicates the column is required and not null.

AUDIT_MGMT_OBLIGATION_ATTRIB table

The **AUDIT_MGMT_OBLIGATION_ATTRIB** table contains information about attributes of the obligations. These obligations are related to Access Management, Person Management, and Account Management that are submitted through the administrative console, Self-service user interface, and the Identity Service Center user interface.

The **AUDIT_MGMT_OBLIGATION_ATTRIB** table contains the following columns.

Table 204. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_ATTRIB** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
OBLIGATION_ID*	Identifier of the obligation to which the resources are related.	Numeric
ATTRIBUTE_NAME*	Name of an attribute that is associated to the obligation.	Character (225)
ATTRIBUTE_VALUE*	Data value of an attribute that is associated to the obligation.	Character (4000)
ATTRIBUTE_PREVIOUS_VALUE	Previously stored data value of an attribute that is associated to the obligation before an edit action.	Character (4000)
SEQUENCE_NO*	A generated numerical value that starts at 1 and increments by 1. It enables the persistence of an attribute name with multiple attribute values.	SMALLINT

* Indicates the column is required and not null.

AUDIT_MGMT_OBLIGATION_RESOURCE table

The **AUDIT_MGMT_OBLIGATION_RESOURCE** table contains information about the obligation resource attributes.

The **AUDIT_MGMT_OBLIGATION_RESOURCE** table contains the following columns.

Table 205. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_RESOURCE** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
OBLIGATION_ID*	Identifier of the obligation to which the resources are related.	Numeric
RESOURCE_TYPE*	The value can be **ACCOUNT**, **PERSON**.	Character (50)
RESOURCE_NAME*	Name of the resource to which access is requested.	Character (1000)
RESOURCE_DN*	Distinguished name of the resource to which access is requested.	Character (1000)

* Indicates the column is required and not null.

AUDIT_MGMT_MESSAGE table

The **AUDIT_MGMT_MESSAGE** table contains messages that are related to access requests. It includes extra audit data that is related to rows in the **AUDIT_EVENT** table for which the **ITIM_EVENT_CATEGORY** column contains the value **AccessRequest**.

The **AUDIT_MGMT_MESSAGE** table contains the following columns.

Table 206. **AUDIT_MGMT_MESSAGE** *table for access request management*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
WORKFLOW_PROCESS_ID*	Identifier of the workflow process to which this additional audit data is related.	Numeric
MESSAGE*	Message that is related to the request.	Character (1000)

* Indicates the column is required and not null.

Note: The **AUDIT_MGMT_MESSAGE** table contains multiple rows that have the same **WORKFLOW_PROCESS_ID** column value if there is more than one message that is associated with the corresponding request.

Values for columns in the AUDIT_EVENT table that is used by access request management

The AUDIT_EVENT table is common for all audit events. However, the value for some columns is different depending on the event. See the specific event for the column values.

Table 207. AUDIT_EVENT table for access request management

Column Name	Column Description	Data type
ID*	ID by which this event is identified. Primary key.	Numeric

Table 207. AUDIT_EVENT table for access request management (continued)

Column Name	Column Description	Data type
ITIM_EVENT_CATEGORY*	**AccessRequest**.	Character (50)
ACTION*	ADD	Character (25)
WORKFLOW_PROCESS_ID	The identifier of the request.	Numeric
INITIATOR_NAME	The user ID of the ITIM account that submitted the request.	Character (1000)
INITIATOR_DN	The distinguished name of the ITIM account that submitted the request.	Character (1000)
INITIATOR_TYPE	PERSON - Indicates that the request was submitted by a person. SYSTEM - Indicates that the request was submitted by the Security Identity Manager system.	Character (50)
INITIATOR_PERSON_DN	Distinguished name of the person who submitted the request.	Character (1000)
INITIATOR_PERSON_NAME	Name of the person who submitted the request.	Character (1000)
RESULT_SUMMARY	The status of the request. The **RESULT_SUMMARY** contains one of the following values. 0 - PENDING 1 - NOT_FULFILLED 2 - PARTIALLY_FULFILLED 3 - FULFILLED	Character (25)
TIMESTAMP*	The time stamp for when the request was submitted.	Character (50)
COMMENTS	The justification for the request.	Character (1000)
TIMESTAMP2	The time stamp for when the request was completed.	Character (50)

* Indicates the column is required and not null.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each IBM Security Identity Manager access request management action in the AUDIT_EVENT table.

Request access event

```
id, itim_event_category, action, workflow_process_id,
initiator_name, initiator_dn, initiator_type, initiator_person_dn,
initiator_person_name, result_summary, timestamp, comments,
timestamp2
```

Manual activity events

This section describes events that are related to manual activities. Some examples of manual activities include approvals, requests for information, and work orders.

In addition to the AUDIT_EVENT table, the AUDIT_MGMT_ACTIVITY and AUDIT_MGMT_PARTICIPANT tables are used by manual activity events

Create manual activity event

The create manual activity event is audited when a manual activity is created.

The following are the manual activities that are created by the system:

Approval
Request for information
Work order
User recertification
Compliance alert
Separation of duty approval

In addition to the AUDIT_EVENT table, create manual activity events use the following tables.

- AUDIT_MGMT_ACTIVITY
- AUDIT_MGMT_PARTICIPANT

AUDIT_MGMT_ACTIVITY table

The **AUDIT_MGMT_ACTIVITY** table contains information about the manual activity that was created and its status.

The **AUDIT_MGMT_ACTIVITY** table contains the following columns.

Table 208. Create manual activity values for the **AUDIT_MGMT_ACTIVITY** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
ROOT_WORKFLOW_PROCESS_ID*	Identifier of the root workflow process in which the manual activity was created.	Numeric
WORKFLOW_PROCESS_ID*	Identifier of the workflow process in which the manual activity was created.	Numeric
ID*	Identifier of the manual activity. The value of this column serves as a foreign key for the **AUDIT_MGMT_ACTIVITY_PARTICIPANT** table.	Numeric
WORKITEM_ID*	Identifier of the work item that represents the current participant assignments and the due date for the manual activity. **Note:** The value of this column is updated when the manual activity is escalated. It then becomes the identifier of the work item that represents the escalation participant assignments and the due date.	Numeric
TYPE*	Type of the activity. APPROVAL COMPLIANCE_ALERT RFI SOD USER_RECERTIFICATION WORK_ORDER	Character (25)
NAME *	Name of the manual activity. The administrator can specify a translated label by using the syntax $labelKey.	Character (1000)
PERSON_NAME *	Name of the person for whom the manual activity was created.	Character (1000)

Table 208. Create manual activity values for the **AUDIT_MGMT_ACTIVITY** *table (continued)*

Column name	Column description	Data type
PERSON_DN	Distinguished name of the person for whom the manual activity was created. The **PERSON_DN** is populated only if the person exists at the time that the activity is created.	Character (1000)
SERVICE_NAME	Name of the service for which the manual activity was created.	Character (1000)
SERVICE_DN	Distinguished name of the service for which the manual activity was created.	Character (1000)
ACCOUNT_USERID	User ID of the account for which the manual activity was created.	Character (1000)
ACCOUNT_DN	Distinguished name of the account for which the manual activity was created. The **ACCOUNT_DN** is populated only if the account exists at the time that the activity was created.	Character (1000)
ACCESS_CATALOG_ID	Identifier of the access catalog item for which the manual activity was created.	Numeric
ACCESS_CATALOG_NAME	Name of the access catalog item for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_DESCRIPTION	Description of the access catalog item for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_CATEGORY	Category of the access catalog item for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_ICON	URL of the access catalog icon for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_BADGE_1	Text and style of the first badge for the access catalog item for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_BADGE_2	Text and style of the second badge for the access catalog item for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_BADGE_3	Text and style of the third badge for the access catalog item for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_BADGE_4	Text and style of the fourth badge for the access catalog item for which the manual activity was created.	Character (1000)
ACCESS_CATALOG_BADGE_5	Text and style of the fifth badge for the access catalog item for which the manual activity was created.	Character (1000)
CREATED_DATE*	Date and time when the manual activity was created.	Character (50)
ESCALATED_DATE	Date and time when the manual activity was escalated. **Note:** This column is not set when the manual activity is created.	Character (50)

*Table 208. Create manual activity values for the **AUDIT_MGMT_ACTIVITY** table (continued)*

Column name	Column description	Data type
DUE_DATE	Date and time when the activity escalates or times out if it is already escalated, or times out if no escalation participants exist. **Note:** This column is updated to set the new due date and time for the escalation participants.	Character (50)
COMPLETED_DATE	Date and time when the manual activity is completed, canceled, or times out. This column is not set when the manual activity is created.	Character (50)
COMPLETION_CODES	Valid completion or result codes for the manual activity.	Character (50)
COMPLETION_CODE	Completion or result code that is specified by the participant when the manual activity is completed. **Note:** This column is not set when the manual activity is created.	Character (50)
STATUS*	Status of the manual activity. APPROVED CANCELED FAILED PENDING REJECTED SKIPPED SUCCESS TIMED_OUT_FAILED TIMED_OUT_SUCCESS WARNING	Character (25)
JUSTIFICATION	Justification that is specified when the user submitted the request that created the manual activity.	Character (4000)
COMMMENTS	Comments that are specified by the participant that completed the activity. This column is not set when the manual activity is created.	Character (1000)

* Indicates the column is required and not null.

Note: The columns for a specified row in the **AUDIT_MGMT_ACTIVITY** table might change as the manual activity changes from one state to another.

- If a participant completes the manual activity, the COMPLETED_DATE column is updated with the date and time that the manual activity was completed. The COMPLETION_CODE column is updated with the completion or result code that is specified by the participant at the time of completion. The COMMENTS column is updated with any comments specified by the participant who completed the activity. The STATUS column is updated accordingly.
- If the manual activity is canceled, skipped, or times out, the COMPLETED_DATE column is updated to contain the date and time of the occurrence. The STATUS column is updated accordingly.

- If the manual activity escalates, the EVENT_ID column remains the unchanged. The WORKITEM_ID column is updated to contain the identifier of the work item that represents the escalation participant assignments and the due date. The ESCALATED_DATE column is updated to contain the date and time when the manual activity was escalated. The DUE_DATE column is updated to contain the new due date for the escalation participant assignments.

AUDIT_MGMT_PARTICIPANT table

The **AUDIT_MGMT_PARTICIPANT** table contains information about participants of manual activities. It includes extra audit data that is related to rows in the **AUDIT_EVENT** table for which the **ITIM_EVENT_CATEGORY** column contains the value **ManualActivity**.

The **AUDIT_MGMT_PARTICIPANT** table contains the following columns.

Table 209. Create manual activity values for the **AUDIT_MGMT_PARTICIPANT** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**.	Numeric
ROOT_WORKFLOW_PROCESS_ID*	Identifier of the root workflow process for the manual activity to which the participant is assigned.	Numeric
WORKFLOW_PROCESS_ID*	Identifier of the workflow process for the manual activity to which the participant is assigned.	Numeric
ACTIVITY_ID*	Identifier of the activity. References **AUDIT_MGMT_ACTIVITY (ID)**.	Numeric
WORKITEM_ID*	Identifier of the work item that represents the current participant assignments and the due date for the manual activity.	Numeric
PERSON_NAME	Name of the person who is a participant of the manual activity.	Character (1000)
PERSON_DN	Distinguished name of the person who is a participant of the manual activity.	Character (1000)
ACCOUNT_USERID	User ID of the IBM Security Identity Manager account that is a participant of the manual activity.	Character (1000)
ACCOUNT_DN	Distinguished name of the IBM Security Identity Manager that is a participant of the manual activity.	Character (1000)
STATUS*	Status of the assignment for the manual activity that is assigned to the participant. CANCELED COMPLETED COMPLETED_OTHER ESCALATED PENDING SKIPPED TIMED_OUT	Character (25)

* Indicates the column is required and not null.

Note: The **AUDIT_MGMT_PARTICIPANT** table contains multiple rows that have the same ACTIVITY_ID column value if there is more than one participant for the corresponding activity.

The rows for a specific **ACTIVITY_ID** might change as the manual activity changes from one state to another:

- Initially the rows represent the original participants for the manual activity.
- If the manual activity escalates, the STATUS column for the original participant rows is updated to ESCALATED. New rows that represent the escalation participants are added with the STATUS column set to PENDING.
- If a participant completes the manual activity, the STATUS column is updated to COMPLETED. Other participants for which the STATUS was PENDING, are updated to COMPLETED_OTHER.
- If the manual activity is canceled or times out, the rows for the participants for which the STATUS is PENDING is updated to CANCELED or TIMED_OUT.

Values for columns in the AUDIT_EVENT table for the create manual activity event

The AUDIT_EVENT table is common for all audit events. However, the value for some columns is different depending on the event. See the specific event for the column values.

Table 210. AUDIT_EVENT table for the create manual activity event

Column Name	Column Description	Data type
ID*	ID by which this event is identified. Primary key.	Numeric
ITIM_EVENT_CATEGORY*	**ManualActivity**.	Character (50)
ACTION*	Create	Character (25)
TIMESTAMP*	The time stamp for when the manual activity was created.	Character (50)

* Indicates the column is required and not null.

Escalate manual activity event

The escalate manual activity event is audited when a manual activity is escalated.

Normal escalation occurs when the activity is not completed by the due date. Escalation also occurs when the participant for the activity cannot be resolved. In this case, the activity is created in an escalated state.

In addition to the AUDIT_EVENT table, escalate manual activity events use the following tables.

- AUDIT_MGMT_ACTIVITY
- AUDIT_MGMT_PARTICIPANT

AUDIT_MGMT_ACTIVITY table

The **AUDIT_MGMT_ACTIVITY** table is modified if a manual activity event is escalated normally or if the participants that are assigned cannot be resolved.

Normal escalation

If the manual activity was not completed by the original participants by the due date and was reassigned to the escalation participants the following columns are changed in the **AUDIT_MGMT_ACTIVITY** table. That table was created when the create manual activity event occurred.

Table 211. Escalate manual activity values for the **AUDIT_MGMT_ACTIVITY** *table*

Column name	Column description	Data type
WORKITEM_ID*	Identifier of the work item that represents the escalation participant assignments and the due date for the manual activity.	Numeric
ESCALATED_DATE	Date and time when the manual activity was escalated. **Note:** This column is not set when the manual activity is created.	Character (50)
DUE_DATE	Date and time when the activity is due or times out. **Note:** This column is updated to set the new due date and time for the escalation participants.	Character (50)

* Indicates the column is required and not null.

Participants cannot be resolved

If the participants for a manual activity cannot be resolved, the activity is created in an escalated state. An example of unresolved participants is an activity that is assigned to a group or role that has no members. The content of the **AUDIT_MGMT_ACTIVITY** table is the same as the create manual activity event with the following modifications.

Table 212. Escalate manual activity values for the **AUDIT_MGMT_ACTIVITY** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that corresponds to the ID column in the AUDIT_EVENT table for the escalate manual activity event.	Numeric
ESCALATED_DATE	Date and time when the manual activity was escalated.	Character (50)
DUE_DATE	Date and time that is set for the escalation participants.	Character (50)

* Indicates the column is required and not null.

AUDIT_MGMT_PARTICIPANT table

The **AUDIT_MGMT_PARTICIPANT** table contains information about participants of manual activities. It includes extra audit data that is related to rows in the **AUDIT_EVENT** table for which the **ITIM_EVENT_CATEGORY** column contains the value **ManualActivity**.

The **AUDIT_MGMT_PARTICIPANT** table contains the following columns.

Table 213. Escalate manual activity event values for the **AUDIT_MGMT_PARTICIPANT** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**.	Numeric
ROOT_WORKFLOW_PROCESS_ID*	Identifier of the root workflow process for the manual activity to which the escalation participant is assigned.	Numeric
WORKFLOW_PROCESS_ID*	Identifier of the workflow process for the manual activity to which the escalation participant is assigned.	Numeric
ACTIVITY_ID*	Identifier of the activity. References **AUDIT_MGMT_ACTIVITY (ID)**.	Numeric
WORKITEM_ID*	Identifier of the work item that represents the escalation participant assignments and the due date for the manual activity.	Numeric
PERSON_NAME	Name of the person who is an escalation participant of the manual activity.	Character (1000)
PERSON_DN	Distinguished name of the person who is an escalation participant of the manual activity.	Character (1000)
ACCOUNT_USERID	User ID of the IBM Security Identity Manager account that is an escalation participant of the manual activity.	Character (1000)
ACCOUNT_DN	Distinguished name of the IBM Security Identity Manager that is an escalation participant of the manual activity.	Character (1000)
STATUS*	Status of the manual activity assignment for the escalation participant. CANCELED COMPLETED COMPLETED_OTHER ESCALATED PENDING SKIPPED TIMED_OUT	Character (25)

* Indicates the column is required and not null.

Note: The **AUDIT_MGMT_PARTICIPANT** table contains multiple rows that have the same ACTIVITY_ID column value if there is more than one participant for the corresponding activity.

The rows for a specific **ACTIVITY_ID** might change as the manual activity changes from one state to another:

- Initially the rows represent the original participants for the manual activity.
- If the manual activity escalates, the STATUS column for the original participant rows is updated to ESCALATED. New rows that represent the escalation participants are added with the STATUS column set to PENDING.
- If a participant completes the manual activity, the STATUS column is updated to COMPLETED. Other participants for which the STATUS was PENDING, are updated to COMPLETED_OTHER.

- If the manual activity is canceled or times out, the rows for the participants for which the STATUS is PENDING is updated to CANCELED or TIMED_OUT.

Values for columns in the AUDIT_EVENT table for the escalate manual activity event

The AUDIT_EVENT table is common for all audit events. However, the value for some columns is different depending on the event. See the specific event for the column values.

Table 214. AUDIT_EVENT table for the escalate manual activity event

Column Name	Column Description	Data type
ID*	ID by which this event is identified. Primary key.	Numeric
ITIM_EVENT_CATEGORY*	**ManualActivity**.	Character (50)
ACTION*	Escalate	Character (25)
TIMESTAMP*	The time stamp for when the manual activity was escalated.	Character (50)

* Indicates the column is required and not null.

Table columns used in the AUDIT_Event table

The following list shows the columns for each IBM Security Identity Manager manual activity event in the AUDIT_EVENT table.

Create manual activity event

```
id, itim_event_category, action, timestamp
```

Escalate manual activity event

```
id, itim_event_category, action, timestamp
```

Lifecycle rule events

When a lifecycle rule is run, information about who submitted the request is audited. If the lifecycle rule creates other root workflow processes, a lifecycle rule event is audited for each created root workflow process.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the lifecycle rule events in the AUDIT_EVENT table.

Table 215. AUDIT_EVENT table for lifecycle rule events

Column Name	Column Description	Data type
ID*	ID by which this event is identified. Primary key.	Numeric
ITIM_EVENT_CATEGORY*	**LifecycleRule**.	Character (50)
ACTION*	Run	Character (25)
WORKFLOW_PROCESS_ID	The identifier of the root workflow process in which the lifecycle is run or its created workflow processes.	Numeric
INITIATOR_NAME	The user ID of the ITIM account that ran the lifecycle rule.	Character (1000)
INITIATOR_DN	The distinguished name of the ITIM account that ran the lifecycle rule.	Character (1000)

Table 215. AUDIT_EVENT table for lifecycle rule events (continued)

Column Name	Column Description	Data type
INITIATOR_TYPE	PERSON - Indicates that the lifecycle rule was run by a person. SYSTEM - Indicates that the lifecycle rule was run by the Security Identity Manager system.	Character (50)
INITIATOR_PERSON_DN	Distinguished name of the person who ran the lifecycle rule.	Character (1000)
INITIATOR_PERSON_NAME	Name of the person who ran the lifecycle rule.	Character (1000)
TIMESTAMP*	The time stamp for when the lifecycle rule was run.	Character (50)

* Indicates the column is required and not null.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each IBM Security Identity Manager lifecycle rule event in the AUDIT_EVENT table.

lifecycle rule

```
id, itim_event_category, action, workflow_process_id,
initiator_name, initiator_dn, initiator_type, initiator_person_dn,
initiator_person_name, timestamp
```

Account management

These AUDIT_EVENT columns are used by events that are related to account management, such as add, modify, suspend, restore, delete, admin change password, password pickup, and adopt.

In addition to the AUDIT_EVENT table, these tables are used by account management events: AUDIT_MGMT_PROVISIONING, AUDIT_MGMT_ACCESS_REQUEST, AUDIT_MGMT_OBLIGATION, AUDIT_MGMT_OBLIGATION_ATTRIB, and AUDIT_MGMT_OBLIGATION_RESOURCE.

AUDIT_MGMT_PROVISIONING table

Table 216. AUDIT_MGMT_PROVISIONING table

Column Name	Column Description	Data type
EVENT_ID*	Identifier assigned to this event. References AUDIT_EVENT (ID).	Numeric
OWNER_NAME	Name of the account owner.	Character (1000)
OWNER_DN	Distinguished name of the owner.	Character (1000)
SERVICE_NAME*	Name of the service to which the account belongs.	Character (1000)
SERVICE_DN*	Distinguished name of the service.	Character (1000)
ACCESS_NAME[1]	Name of the access type that the account acquired.	Character (1000)
ACCESS_DN[1]	Distinguished name of the access type.	Character (1000)

* Indicates the column is required and not null.

[1] Indicates the column was added in release 5.0.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the account management events in the AUDIT_EVENT table.

Table 217. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Account Management.
entity_name	Name of the account.
entity_dn	Distinguished name of the account.
entity_type	Types of the account (service). For example, Active Directory, Oracle, LDAP, Windows 2000, or IBM Security Identity Manager.
action	Types of actions: Add – Provision a new account on the target resource Modify – Modify an existing account Delete – Delete existing account Suspend – Suspend existing account Restore – Restore existing account ChangePassword – Change password for an account PasswordPickup – Pick a password for an account identified by the provisionTarget Adopt – Adopt an orphan account Orphan – Orphan an account

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each account management event in the AUDIT_EVENT table.

- **Add Account event**

  entity_name, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_provisioning: owner_name, owner_dn, service_name, service_dn

- **Modify Account event**

  entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_provisioning: owner_name, owner_dn, service_name, service_dn

- **Delete Account event**

  entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_provisioning: owner_name, owner_dn, service_name, service_dn

- **Suspend Account event**

entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

From audit_mgmt_provisioning: owner_name, owner_dn, service_name, service_dn

- **Restore Account event**

  entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_provisioning: owner_name, owner_dn, service_name, service_dn

- **Change Password event**

  entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_provisioning: owner_name, owner_dn, service_name, service_dn

- **Synchronize Password event**

  entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

  From audit_mgmt_provisioning: owner_name, owner_dn, service_name, service_dn

- **Adopt Account event**

  entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

  From audit_mgmt_provisioning: owner_dn, service_dn

- **Orphan Account event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

  From audit_mgmt_provisioning: owner_dn, service_dn

Table columns for account management in the AUDIT_MGMT_ACCESS_REQUEST table

The following list shows the columns for all account management event in the AUDIT_MGMT_ACCESS_REQUEST table.

- Event_ID
- Wokflow_Process_Id
- Action
- Access_Obligations_Ids
- Status
- Completed_Date
- Person_Name
- Person_DN

Table columns for account management in the AUDIT_MGMT_OBLIGATION table

The following list shows the columns for all account management event in the AUDIT_MGMT_OBLIGATION table.

- Event_ID
- Id
- Person_Dn
- Obligation_Type
- System_Generated

AUDIT_MGMT_OBLIGATION_ATTRIB table

The **AUDIT_MGMT_OBLIGATION_ATTRIB** table contains information about attributes of the obligations. These obligations are related to Access Management, Person Management, and Account Management that are submitted through the administrative console, Self-service user interface, and the Identity Service Center user interface.

The **AUDIT_MGMT_OBLIGATION_ATTRIB** table contains the following columns.

Table 218. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_ATTRIB** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric
OBLIGATION_ID*	Identifier of the obligation to which the resources are related.	Numeric
ATTRIBUTE_NAME*	Name of an attribute that is associated to the obligation.	Character (225)
ATTRIBUTE_VALUE*	Data value of an attribute that is associated to the obligation.	Character (4000)
ATTRIBUTE_PREVIOUS_VALUE	Previously stored data value of an attribute that is associated to the obligation before an edit action.	Character (4000)
SEQUENCE_NO*	A generated numerical value that starts at 1 and increments by 1. It enables the persistence of an attribute name with multiple attribute values.	SMALLINT

* Indicates the column is required and not null.

AUDIT_MGMT_OBLIGATION_RESOURCE table

The **AUDIT_MGMT_OBLIGATION_RESOURCE** table contains information about the obligation resource attributes.

The **AUDIT_MGMT_OBLIGATION_RESOURCE** table contains the following columns.

Table 219. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_RESOURCE** *table*

Column name	Column description	Data type
EVENT_ID*	Identifier that is assigned to this event. References **AUDIT_EVENT (ID)**	Numeric

Table 219. **AccessRequest** *values for the* **AUDIT_MGMT_OBLIGATION_RESOURCE** *table (continued)*

Column name	Column description	Data type
OBLIGATION_ID*	Identifier of the obligation to which the resources are related.	Numeric
RESOURCE_TYPE*	The value can be **ACCOUNT**, **PERSON**.	Character (50)
RESOURCE_NAME*	Name of the resource to which access is requested.	Character (1000)
RESOURCE_DN*	Distinguished name of the resource to which access is requested.	Character (1000)

* Indicates the column is required and not null.

Container management

This section describes the columns used by events related to events specific to container management, such as add, modify, and delete.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the container management operations in the AUDIT_EVENT table.

Table 220. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Container Management.
entity_name	Name of the container.
entity_dn	Distinguished name of the container.
entity_type	Types of entities: Organization Org_unit Business_Partner_Organization Location Admin_Domain
action	Types of actions: Add – Add a container Modify – Modify an existing container Delete – Delete a container

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management action in the AUDIT_EVENT table.

- **Add Container event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Container event**

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Delete Container event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

Organization role management

This section describes the columns used by events related to organization role management, such as add, modify, and delete.

In addition to the AUDIT_EVENT table, the AUDIT_MGMT_TARGET table is used by organization role management events.

AUDIT_MGMT_TARGET table

The AUDIT_MGMT_TARGET table is used if the action is Add Member or Remove Member.

Table 221. AUDIT_MGMT_TARGET table

Column Name	Column Description	Value Type	Required?
event_id	Identifier for the event. Foreign key to the ID column of the table audit_event.	long	Yes
target_entity_name	The name of the member that is being added to or removed from the role. Applicable if action= Add Member/ Remove Member.	string	Yes, when action= Add Member or Remove Member
target_entity_dn	The distinguished name of the member that is being added to or removed from the role. Applicable if action= Add Member/ Remove Member.	string	Yes, when action= Add Member or Remove Member
target_entity_type	The type of the member that is being added to or removed from the role. Applicable if action= Add Member/ Remove Member.	string	Yes, when action= Add Member or Remove Member

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the organization role management events in the AUDIT_EVENT table.

Table 222. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Organizational Role Management
entity_name	Name of the role.
entity_dn	Distinguished name of the role.
entity_type	Types of entities: static_org_role – Static organizational role that is involved in this event. dynamic_org_role – Dynamic organizational role that is involved in this event.

Table 222. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
action	Types of actions: Add – Add a role. Modify – Modify an existing role. This action also involves modifying membership. Delete – Delete a role. AddMember – Add a member to the role. RemoveMember – Remove a member from the role.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each organization role management event in the AUDIT_EVENT table.

Add Static Role event

entity_name, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Modify Static Role event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Delete Static Role event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Add Member to Static Role event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, timestamp, result_summary

AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn, target_entity_type

Remove Member from Static Role event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, timestamp, result_summary

AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn, target_entity_type

Add Dynamic Role event

entity_name, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Modify Dynamic Role event

entity_name, entity_dn, entity_type, workflow_process_id,

initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Delete Dynamic Role event

entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

ITIM group management

These AUDIT_EVENT columns are used by events that are related to ITIM group management, such as add, modify, and delete.

In addition to the AUDIT_EVENT table, the AUDIT_MGMT_TARGET table is used by ITIM group management events.

AUDIT_MGMT_TARGET table

The AUDIT_MGMT_TARGET table is used if the action is Add Member or Remove Member.

Table 223. AUDIT_MGMT_TARGET table

Column Name	Column Description	Value Type	Required?
event_id	Identifier associated with this event. Foreign key to the ID column of the table audit_event.	long	Yes
target_entity_name	The name of the member that is being added to or removed from the ITIM group. Applicable if action= Add Member or Remove Member.	string	Yes, when action= Add Member or Remove Member
target_entity_dn	The distinguished name of the member that is being added to or removed from the ITIM group. Applicable if action= Add Member or Remove Member.	string	Yes, when action= Add Member or Remove Member
target_entity_type	The type of the member that is being added to or removed from the ITIM group. Applicable if action= Add Member or Remove Member.	string	Yes when action= Add Member or Remove Member

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the ITIM group management events in the AUDIT_EVENT table.

Table 224. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	ITIM Group Management
entity_name	Name of the ITIM group.
entity_dn	Distinguished name of the ITIM group.

Table 224. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
entity_type	Types of entities: static_org_role – Static organizational role that is involved in this event. dynamic_org_role – Dynamic organizational role that is involved in this event.
action	Types of actions: Add – Add an ITIM group. Modify – Modify an ITIM group. This action also involves modifying membership. Delete – Delete an ITIM group. AddMember – Add a member to the ITIM group. RemoveMember – Remove a member from the ITIM group.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each ITIM group management event in the AUDIT_EVENT table.

Add ITIM Group event

entity_name, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Modify ITIM Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Delete ITIM Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Add Member to ITIM Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, timestamp, result_summary

AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn, target_entity_type

Remove Member from ITIM Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, workflow_process_id, timestamp, result_summary

AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn, target_entity_type

Service management

This section describes the columns used by event-specific to service, such as add, modify, and delete.

In addition to the AUDIT_EVENT table, the AUDIT_MGNT_TARGET table is used by account management events.

AUDIT_MGNT_TARGET table

Table 225. AUDIT_MGNT_TARGET table

Column Name	Column Description	Value Type	Required?
event_id	Identifier associated with this event. Foreign key to the ID column of the table audit_event.	long	Yes
target_entity_name	Name of the target (service, service profile, or all services) for the adoption rule. Applicable if action= Add, Modify, or Delete an adoption rule.	string	Yes for action= Add, Modify, or Delete an adoption rule
target_entity_dn	The distinguished name of the target (service, service profile, or all services) for adoption rule. Applicable if action= Add, Modify, or Delete an adoption rule.	string	Yes for action= Add, Modify, or Delete an adoption rule
target_entity_type	The type of the target (service, service profile, or all services) for adoption rule. Applicable if action= Add, Modify, or Delete an adoption rule.	string	Yes for action= Add, Modify, or Delete an adoption rule

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the container management operations in the AUDIT_EVENT table.

Table 226. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Service Management.
entity_name	Name of the service.
entity_dn	Distinguished name of the service.
entity_type	Types of resource the service represents. For example: Active Directory, Oracle, LDAP, Windows 2000, or IBM Security Identity Manager.
action	Types of actions: Add – Add a service. Modify – Modify a service. This action includes the change compliance alert operation. Delete – Delete a service. Add_adoption_rule – Add an adoption rule for this service group. Update_adoption_rule – Update adoption rule for this service/service type. Delete_adoption_rule – Delete adoption rule for this service/service type.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management action in the AUDIT_EVENT table.

- **Add Service event**

entity_name, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Modify Service event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Delete Service event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Add Adoption rule Service event**

  entity_name, entity_dn, initiator_name, initiator_dn, timestamp, result_summary

  AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn

- **Modify Adoption rule Service event**

  entity_name, entity_dn, initiator_name, initiator_dn, timestamp, result_summary

  AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn

- **Delete Adoption rule Service event**

  entity_name, entity_dn, initiator_name, initiator_dn, timestamp, result_summary

  AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn

Group management

This section describes the tables that are used by events that are related to group, such as add, modify, and delete.

In addition to the AUDIT_EVENT table, the AUDIT_MGMT_TARGET table is used by group management events.

AUDIT_MGMT_TARGET table

The AUDIT_MGMT_TARGET table is used if the action is Add Member or Remove Member.

Table 227. AUDIT_MGMT_TARGET table

Column Name	Column Description	Value Type	Required?
event_id	Identifier that is associated with this event. Foreign key to the ID column of the table audit_event.	long	Yes
target_entity_name	The name of the member that is being added to or removed from the group. Applicable if action= Add Member or Remove Member.	string	Yes, when action= Add Member or Remove Member
target_entity_dn	The distinguished name of the member that is being added to or removed from the group. Applicable if action= Add Member or Remove Member.	string	Yes, when action= Add Member or Remove Member
target_entity_type	The type of the member that is being added to or removed from the group. Applicable if action= Add Member or Remove Member.	string	Yes when action= Add Member or Remove Member

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the group management events in the AUDIT_EVENT table.

Table 228. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Group Management
entity_name	Unique identifier of the group. This identifier can be the group ID or name.
entity_dn	Distinguished name of the group.
entity_type	Types of the group. For example: LdapGroupProfile, PosixAixGroupProfile.
container_name	Name of the service that holds the group.
container_dn	Distinguished name of the service that holds the group.
action	Types of actions: Add – Add a group. Modify – Modify a group. Delete – Delete a group. AddMember – Add a member to a group. RemoveMember – Remove a member from a group.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each group management event in the AUDIT_EVENT table.

Add Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Modify Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Delete Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

Add Member to Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn, target_entity_type

Remove Member from Group event

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, container_name, container_dn, timestamp, result_summary

AUDIT_MGMT_TARGET table: target_entity_name, target_entity_dn, target_entity_type

Service policy enforcement

This section describes the columns used by service policy enforcement events such as mark, correct, suspend, and alert.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the service policy enforcement events in the AUDIT_EVENT table.

Table 229. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	service_policy_enforcement
entity_name	Name of the service.
entity_dn	Distinguished name of the service.
entity_type	Type of the resource the service represents. For example: Active Directory, Oracle, LDAP, Windows 2000, or IBM Security Identity Manager.
action	Types of actions: EnforcePolicyForService - Enforce policy compliance MarkNonCompliant – Mark noncompliant accounts. SuspendNonCompliant – Suspend noncompliant accounts. CorrectNonCompliant – Correct noncompliant accounts. AlertNonCompliant – Alert the participant. UseGlobalSetting – Issues the action that is specified in global setting.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each service policy enforcement event in the AUDIT_EVENT table.

Service Policy Enforcement action event

entity_name, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, action, container_name, container_dn, timestamp, result_summary

Set Global Policy Enforcement properties event

entity_name, entity_dn, entity_type, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, action, container_name, container_dn, timestamp, result_summary

Reconciliation

This section describes the columns used by events specific to reconciliation, such as runRecon, setServiceParams, and setReconUnit.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the reconciliation events in the AUDIT_EVENT table.

Table 230. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Reconciliation.
entity_name	Name of the service.
entity_dn	Distinguished name of the service.
entity_type	Type of the resource the service represents. For example: Active Directory, Oracle, LDAP, Windows 2000, or IBM Security Identity Manager.
action	Types of actions: Runrecon – Start the reconciliation. SetServiceReconParameters – Set the service reconciliation parameters. SetReconUnit – Set the service reconciliation unit.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each reconciliation event in the AUDIT_EVENT table.

Run Reconciliation event

```
entity_name, entity_dn, entity_type, workflow_process_id,
initiator_name, initiator_dn, initiator_type, initiator_person_dn,
initiator_person_name, action, timestamp, result_summary
```

Set Recon Unit event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
action, timestamp, result_summary
```

Set Service Recon Parameters event

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
action, timestamp, result_summary
```

Entitlement workflow management

This section describes the columns used by events specific to custom workflow management, such as add, modify, and delete.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the container management operations in the AUDIT_EVENT table.

Table 231. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Entitlement Workflow management.
entity_name	Name of the workflow.
entity_dn	Distinguished name of the workflow.

Table 231. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
entity_type	Types of entities: global – Applied to any policy regardless of the service type *service_type* – Type of service to which this workflow is applicable
action	Types of actions: Add – Add a workflow. Modify – Update a workflow. Delete – Delete a workflow.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management action in the AUDIT_EVENT table.

- **Add Entitlement workflow event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Delete Entitlement workflow event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Modify Entitlement workflow event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

Entity operation management

This section describes the columns used by events specific to system workflow management, such as add, modify, and delete.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the container management operations in the AUDIT_EVENT table.

Table 232. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Entity Operation Management.
entity_name	Name of the operation that is being managed.
entity_dn	Distinguished name of the workflow.
entity_type	Type of the entity whose operation is being managed. For example, Person, Account, Bpperson, ITIMAccount, SQLAccount, and others.
action	Types of actions: Add – Add an operation. Modify – Update an operation. Delete – Delete an operation.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management action in the AUDIT_EVENT table.

- **Add Entity Operation event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

- **Delete Entity Operation event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

- **Modify Entity Operation event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

System configuration

This section describes the columns used by events specific to IBM Security Identity Manager configuration performed through the Configuration tab.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the container management operations in the AUDIT_EVENT table.

Table 233. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	IBM Security Identity Manager System Configuration.
entity_name	Name of the entity. The value is specific to the type of entity type that is being updated.
entity_dn	Distinguished name of the entity or entity type if the entity that is being updated is an attribute.
entity_type	Types of entity: FormTemplate – Formtemplate for IBM Security Identity Manager object profiles JoinDirective – Policy join directives ComplianceAlertRule – Policy compliance alert rule (Privilege rule) LogonProperties – Security Identity Manager logon properties PolicyEnforcementProperties – Policy enforcement properties PostOfficeConfigurationProperties – Post Office configuration properties WorkflowNotificationProperties – Workflow notification properties ChallengeResponseProperties – Security Identity Manager challenge and response properties Serviceprofile – Service profile *ITIM System Entity* - System defined entities. For example, Person, Account, BPperson, Organization, BPOrganization, ITIMAccount, SQLAccount, and others.

Table 233. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
action	Types of actions: Add – Add a property or system entity from the Configuration tab. Modify – Update a property or system entity from the Configuration tab. Delete – Delete a property or system entity from the Configuration tab.

Value of the entity_name column

This section describes the value for the entity_name column for each entity_type value defined for system configuration events.

Table 234. Value of the entity_name column table

entity_type	Value	Example
FormTemplate	Name of the profile whose form is being modified.	Admin Domain, Person, AIX Account, DSML2Service, SQLService, Organization
JoinDirective	Name of the attribute whose join directive is being updated.	Errole, eruid, erhomepage
Compliance Alert Rule	Name of the attribute whose Compliance alert rule is being updated.	Errole, eruid, erhomepage
LogonProperties	Property name.	erLostPswdByMail, erResponseEmail, erNumLogonAttempt
Policy Enforcement Properties	Property name.	
Post Office Configuration Properties	Property name.	
Workflow Notification Properties	Property name.	
Challenge Response Properties	Property name.	erChallengeDefMode, erChallengeMode, erResponseEnable
ITIM System Entity	Attribute of the entity that is being updated.	erAttrMap, erSearchAttr, erCustomClass, erRdnAttr, erLifeCycleRule.
Serviceprofile	Name of the service profile that is being installed or uninstalled.	Win2kService, BroadVisionService, SolarisService

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management action in the AUDIT_EVENT table.

- **Add System Entity event**

  entity_name, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

- **Delete System Entity event**

  entity_name, entity_dn, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

- **Modify System Entity event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

- **Add Life Cycle Rule event**

  entity_name, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Delete Life Cycle Rule event**

  entity_name, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Modify Life Cycle Rule event**

  entity_name, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Challenge Config event**

  initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Challenges event**

  initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Form Template event**

  entity_name, entity_dn, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Password Properties event**

  initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Post Office Properties event**

  initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Privilege Rule event**

  entity_name, entity_dn, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Workflow Notification Properties event**

  initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary
- **Set Workflow Notification Template event**

  entity_name, entity_dn, initiator_name, initiator_dn, action, container_name, container_dn, timestamp, result_summary

Runtime events

This section describes the columns used by event related to IBM Security Identity Manager start and stop events.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the container management operations in the AUDIT_EVENT table.

Table 235. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	IBM Security Identity Manager runtime events.

Table 235. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
action	Types of actions: Start_itim – Start command for Security Identity Manager. MStop_itim – Stop command for Security Identity Manager.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each person management action in the AUDIT_EVENT table.

- **Start ITIM Server event**

  action, timestamp, result_summary
- **Stop ITIM Server event**

  action, timestamp, result_summary

Self-password change

This section describes the columns that are used by events that are related to password change.

If a self-password change request affects at least one ITIM account and at least one non-ITIM account, two separate events are audited for the request. One self-password change event is audited for the ITIM accounts. Another self-password change event is audited for the non-ITIM accounts.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the self-password change events in the AUDIT_EVENT table.

Table 236. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Self-password change.
action	Types of actions: ChangePassword – Changing a self-password. ResetPassword – Resetting a self-password.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each self-password change event in the AUDIT_EVENT table.

Change self-password event

entity_name, entity_dn, action, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

Reset self-password event

entity_name, entity_dn, action, workflow_process_id, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

Migration

This section describes the columns used by events related to migration (import and export) operations.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the migration events in the AUDIT_EVENT table.

Table 237. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	Migration.
action	Types of actions: StartImport StopImport StartExport StopExport InstallAgentProfile

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each migration event in the AUDIT_EVENT table.

Start Import event

Event_category, operation, action, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

Stop Import event

Event_category, operation, action, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

Start Export event

Event_category, operation, action, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

Stop Export event

Event_category, operation, action, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

Agent Profile Install event

Event_category, operation, action, initiator_name, initiator_dn, initiator_type, initiator_person_dn, initiator_person_name, timestamp, result_summary

Credential management

This section describes the columns used by events related to Credential management. For example, add to vault, modify, delete, register password, view password history, or get password for non-exclusive credential.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the Credential management operations in the AUDIT_EVENT table.

Table 238. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	CredentialManagement
entity_name	Credential name.
entity_dn	Distinguished name of the credential.
entity_type	Credential
workflow_process_id	Process ID of the initiated workflow. Only applicable to Add action.
result_summary	Result of operation: Submitted – submitted to workflow successfully Success – completed successfully
action	Types of actions: Add – add a credential to vault Modify – modify a credential Delete – delete a credential from vault RegisterPassword – register credential password in the vault PasswordHistory – view credential password history in the vault GetPassword – get password of non-exclusive credential from vault Connect – connect a credential to an account

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each Credential management action in the AUDIT_EVENT table.

- **Add to Vault event**

  entity_name, entity_type, initiator_name, initiator_dn, workflow_process_id, container_name, container_dn, timestamp, result_summary, comments
- **Delete Credential event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary
- **Modify Credential event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary
- **Register Password event**

entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **View Password History event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Get Password event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Connect credential event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, workflow_process_id, container_name, container_dn, timestamp, result_summary, comments

Credential Pool management

This section describes the columns used by events related to Credential Pool management, such as add, modify, or delete.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the Credential Pool management operations in the AUDIT_EVENT table.

Table 239. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	CredentialPoolManagement
entity_name	Credential pool name.
entity_dn	Distinguished name of the credential pool.
entity_type	CredentialPool
result_summary	Result of operation: Success – completed successfully
action	Types of actions: Add – add a credential pool Modify – modify a credential pool Delete – delete a credential pool

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each Credential Pool management action in the AUDIT_EVENT table.

- **Add Credential Pool event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Delete Credential Pool event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

- **Modify Credential Pool event**

```
entity_name, entity_dn, entity_type, initiator_name, initiator_dn,
container_name, container_dn, timestamp, result_summary
```

Credential Lease management

This section describes the columns used by events related to Credential Lease management. For example, check out, check in, get password, notify expired lease, or notify and check in expired lease.

AUDIT_MGMT_LEASE table

The AUDIT_MGMT_LEASE table is used in the following events.

The events are:

- Checkout event
- All other events if the credential is a pool member

Table 240. AUDIT_MGMT_LEASE table

Column Name	Column Description	Data type
event_id*	Identification assigned to the event. References AUDIT_EVENT (ID).	Numeric
lease_expiration_date	The lease expiration time. Only applicable to the Checkout action.	Character (500)
justification	The business justification for checkout. Only applicable to the Checkout action.	Character (2000)
pool_name	The credential pool name. Applicable to all actions if the credential is a pool member.	Character (256)
pool_dn	The credential pool DN. Applicable to all actions if the credential is a pool member.	Character (2000)
custom_attribute_1 to custom_attribute_5	The lease custom attribute values. Only applicable to the Checkout action.	Character (2000)
lease_dn	The lease DN.	Character (2000)

* Indicates the column is required and not null.

Values for columns in the AUDIT_EVENT table

The following table describes the column values for the Credential Lease management operations in the AUDIT_EVENT table.

Table 241. Values for columns in the AUDIT_EVENT table

Column Name	Value
itim_event_category	CredentialLeaseManagement
entity_name	Credential name.
entity_dn	Distinguished name of the credential.
entity_type	Credential
workflow_process_id	Process ID of the initiated workflow. Applicable to Checkin, Checkout, NotifyExpiredLease, and NotifyCheckinExpiredLease actions.

Table 241. Values for columns in the AUDIT_EVENT table (continued)

Column Name	Value
result_summary	Result of operation: Submitted – submitted to workflow successfully. Success – completed successfully. Only applicable to GetPassword action. Failure – failed. Only applicable to the second Checkin event, which tries to check in a credential already checked in by someone else.
action	Types of actions: Checkout – check out a credential. Checkin – check in a credential. GetPassword – get password of a checked out credential. NotifyExpiredLease – Notify an expired lease. NotifyCheckinExpiredLease – Notify and check in an expired lease.

Table columns used in the AUDIT_EVENT table

The following list shows the columns for each Credential Lease management action in the AUDIT_EVENT table.

- **Checkout event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, workflow_process_id, container_name, container_dn, timestamp, result_summary

  AUDIT_MGMT_LEASE table: lease_expiration_time, justification, pool_name, pool_dn, custom_attribute_1, custom_attribute_2, custom_attribute_3, custom_attribute_4, custom_attribute_5

- **Checkin event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, workflow_process_id, container_name, container_dn, timestamp, result_summary, comments

  Note: If a user or an IBM Security Access Manager ESSO session tries to check in a credential already checked in by someone else, then the second checkin attempt is audited as a Checkin event. The result_summary is FAILURE and the comment is Invalid lease during checkin.

  AUDIT_MGMT_LEASE table: pool_name, pool_dn, lease_dn

- **Get Password event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, container_name, container_dn, timestamp, result_summary

  AUDIT_MGMT_LEASE table: pool_name, pool_dn

- **Notify Expired Lease event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, workflow_process_id, container_name, container_dn, timestamp, result_summary

  AUDIT_MGMT_LEASE table: pool_name, pool_dn

- **Notify and Checkin Expired Lease event**

  entity_name, entity_dn, entity_type, initiator_name, initiator_dn, workflow_process_id, container_name, container_dn, timestamp, result_summary

  AUDIT_MGMT_LEASE table: pool_name, pool_dn, lease_dn

Chapter 4. IBM Cognos reporting query subjects and query items

You can use the query subjects and query items to customize the reports.

IBM Cognos reporting model is broadly dived into audit and configuration namespaces.

Audit namespace
Consists of the query subjects and query items for the audit activities.

Configuration namespace
Consists of the query subjects and query items for the configuration activities.

Schema mapping

Before you work with the query subjects and query items, you must map the attributes to the entities.

To map the attributes and entities, see "Mapping the attributes and entities."

For more information, see Report schema mapping

Mapping the attributes and entities

You must map the following attributes to the entities to work with the query items for the IBM Security Identity Manager Cognos report models.

Note: After you map the schema by using IBM Security Identity Manager administration console, it might take some time to reflect the updated data in the Cognos report. You must run a successful data synchronization after mapping the attributes. You must restart IBM Cognos Business Intelligence server to reflect the updated schema in the report.

Table 242. Mapping the attributes and entities

Namespace	Entity	Attribute Name
Account Configuration	Organizational Role	• Access Name • Object Profile Name
	Identity Policy	• Policy Name • Policy Target • Enabled • Scope • UserClass
	Password Policy	• Policy Name • Policy Target • Enabled • Scope
	Account	Account Ownership Type

Table 242. Mapping the attributes and entities (continued)

Namespace	Entity	Attribute Name
Role Configuration	Organizational Role	• Access Name • Access Options • Object Profile Name • Owner
Provisioning Policy Config	Provisioning Policy	• Enabled • Entitlement Ownership Type • Priority • Scope
Shared Access Audit	Account	Account Ownership Type
Shared Access Configuration	Account	Account Ownership Type
	Group	Group Name
Recertification Audit	Account	Account Ownership Type
Recertification Config	Account	Account Ownership Type
	Group	• eraccessdescription • Group Description • Group Name
	Recertification Policy	Scope
User Configuration	Account	Account Ownership Type
	Person	• Administrative Assistant • Preferred user ID • Email Address • Aliases
	Organizational Role	• Access Name • Access Options • Object Profile Name • Owner
	Business Partner Person	• Organization Role • Status
Service Audit	Service	Tag
	Provisioning Policy	• Enabled • Priority • Scope
Access Audit	Group	• Access Options • Group Name
	Organizational Role	• Access Name • Object Profile Name
Access Configuration	Business Partner Person	• Full Name • Last Name • Organizational Unit Name

Recertification Audit namespace

The Recertification Audit namespace provides information about the history of user, role, account, and group recertification.

Query subjects for Recertification Audit namespace

The following table lists the query subjects in the Recertification Audit namespace.

Table 243. Query subjects in the Recertification Audit namespace for the recertification model

Query subject	Description
User Recertification Policy	Represents the recertification policy that recertifies accounts, group memberships, and roles memberships through user recertification. IBM Security Identity Manager entities are recertified with the recertification policy. You must use this query subject with the User Recert History query subject to obtain information about the recertification policy. Do not use this query subject with Account Recert History and Access Recert History.
User Recert History	Represents the recertification audit history for a user. It covers recertification audit history of accounts, groups, and roles that are associated with the user.
Person	Represents a user entity and some of its configuration attributes. You must use this query subject with the User Recert History query subject to obtain information about the user that is being recertified.
Person Organization	Represents an organization that is associated with a user. These users are being recertified.
User Recert Account	Represents the recertification audit history for an account that is recertified as part of the user recertification. You must use this query subject with the User Recert History. By doing so, you can obtain the information about accounts that are associated with the users that are being recertified.
User Recert Group	Represents the recertification audit history for a group membership that is recertified as part of the user recertification. You must use this query subject with the User Recert History. By doing so, you can obtain the information about memberships of the accounts that are associated with the users that are being recertified.
User Recert Group Service	Represents the service that is associated to a group. You must use this query subject with the User Recert History to obtain more information about the service for the groups that are recertified as a part of the user recertification.
User Recert Role	Represents the recertification audit history for a role membership that is recertified as part of the user recertification. You must use this query subject with the User Recert History. By doing so, you can obtain the information about role memberships of the users that are being recertified.
Account	Represents an account entity and some of its configuration attributes. You must use this query subject with the Account Recert History query subject. By doing so, you can generate recertification history reports of accounts.
Account Service	Represents service that is associated to an account. These accounts participate in the account and access recertification.
Account Owner	Represents user owners of the accounts that are participating in the account and access recertification.
Account Recert History	Represents the recertification audit history for accounts. You must use this query subject with the Account query subjects. By doing so, you can find out the accounts in the recertification audit.
Access	Represents the group access and some of its configuration attributes. You must use this query subject with the Access Recert History query subject to generate recertification history reports of access.
Access Recert History	Represents the recertification audit history for access. You must use this query subject with the Access query subjects. By doing so, you can find out the accesses in the recertification audit.

Query items for Recertification Audit namespace

The following table lists the query items in the Recertification Audit namespace.

Table 244. Query items in the Recertification Audit namespace

Query subject	Query items and their description
User Recertification Policy	**Recertification Policy Name** The name of the recertification policy. **Recertification Policy Type** The type of an entity that gets recertified by using this policy. The valid values are Account, Access, and Identity. **Recertification Policy Description** The description of the policy as specified in the policy configuration. **Recertification Policy Enabled** Shows whether the policy is enabled. **Recertification Policy Scheduled** The recertification scheduling modes. The valid values are CALENDAR and ROLLING. **Recertification Policy Rolling Interval in Days** The recertification period if the recertification policy scheduling mode is ROLLING. No value in this query item indicates that the scheduling is not in the ROLLING mode. **Recertification Policy Reject Action** An action that was taken if the recertification is rejected. **Recertification Policy Timeout Period in Days** The duration during which a recertifier must act. **Recertification Policy Timeout Action** The automatic action that must be taken if the recertification times out. **Recertification Policy DN** An LDAP distinguished name for the recertification policy. **Recertification Policy Container DN** An LDAP distinguished name for a business unit to which the recertification policy applies. **Recertification Policy Is Custom** Indicates whether the recertification policy is customized. It is defined in the workflow. **Recertification Policy User Class** The type of a user to which the recertification policy applies. The valid values are All, Person, and Business Partner Person. **Recertification Policy Scope** Indicates whether the recertification policy applies to the business unit and its subunits or either of them.

Table 244. Query items in the `Recertification Audit` namespace (continued)

Query subject	Query items and their description
User Recert History	**User Recert History Person Name** The full name of a person. **User Recert History Person Email** The user email identifier. **User Recert History Person Status** A user status at the end of the recertification workflow process. The valid values are `Active` and `Inactive`. **User Recert History Person Business Unit Name** A business unit to which a user belongs. **User Recert History Recertification Policy Name** The recertification policy that created a user entity. **User Recert History Timeout** Shows whether the recertification process is timed out or not. `0` represents `Not timed out`, and `1` represents `Timed out`. **User Recert History Comments** The comments that are entered by a user during the user recertification process. **User Recert History Process Comments** The comments that are entered by a user during the recertification process. **User Recert History Process Submission time** The recertification policy submission time. **User Recert History Process Start Time** The time at which user recertification workflow process was started. **User Recert History Process Completion Time** A user recertification history process completion time. **User Recert History Process Last Modified Time** The time at which user recertification workflow process was last modified. **User Recert History Process Requester Name** The name of a user who submitted the request for recertification. **User Recert History Process Requestee Name** The name of a user entity for whom the request for recertification was submitted. **User Recert History Process Recertifier Name** The name of a user who is the final approver in the recertification workflow process. **User Recert History Process Result Summary** An overall summary of a user recertification workflow process result. **User Recert History Process Scheduled** The schedule for recertification policy submission. **User Recert History Id** A unique ID assigned by the IBM Security Identity Manager to a user recertification audit history. **User Recert History Person DN** An LDAP distinguished name for a user entity in the recertification process. **User Recert History Recertification Policy DN** An LDAP distinguished name for the recertification policy that recertifies a user entity.

Table 244. Query items in the `Recertification Audit` namespace (continued)

Query subject	Query items and their description
Person	**Person Full Name** The full name of a user. **Person Last Name** The surname of a user. **Person Status** The status of a user. **Person Dn** An LDAP distinguished name for a user entity. **Person Business Unit Dn** An LDAP distinguished name for a business unit to which a user belongs. **Person Supervisor** The name of a user who is the supervisor of a user entity.
Person Organization	**Business Unit Name** The name of a business unit to which a user belongs. **Business Unit Supervisor** A user supervisor of a business unit. **Business Unit DN** An LDAP distinguished name for the business unit to which a user belongs. **Business Unit Container DN** An LDAP distinguished name for the parent business unit of an organization entity.
User Recert Account	**User Recert Account Name** The name of an account in a user recertification. **User Recert Account Service Name** The name of a service to which an account belongs. **User Recert Account Service Description** Describes the service that is associated to an account. **User Recert Account Status** The status of an account at the end of the recertification. The valid values are `Approved` and `Rejected`. **User Recert Account Recert Id** A unique numeric ID assigned by the IBM Security Identity Manager to an account recertification. **User Recert Account DN** An LDAP Distinguished name for an account entity in the recertification. **User Recert Account Service DN** An LDAP Distinguished name for the service to which an account entity belongs.

Table 244. Query items in the `Recertification Audit` namespace (continued)

Query subject	Query items and their description
User Recert Group	**User Recert Group Name** The name of a group in the user recertification. **User Recert Group Description** Describes the recertification group. **User Recert Group Status** The status of a group at the end of the recertification. The valid values are `Approved` and `Rejected`. **User Recert Group Recert Id** A unique numeric ID assigned by IBM Security Identity Manager to a group recertification. **User Recert Group DN** An LDAP Distinguished name for a group entity in the recertification.
User Recert Group Service	**Group Name** The name of a group. **Service Name** The name of a service to which the group belongs. **Service Type** The service profile type. **Service Url** A URL that connects to the managed resource. **Service DN** An LDAP distinguished name for a service to which the group belongs. **Service Container Dn** An LDAP distinguished name for a business unit of the service that is associated with a group. **Service Owner Dn** An LDAP distinguished name for a user owner of the service. **Group Dn** An LDAP distinguished name for a group entity in the recertification.
User Recert Role	**User Recert Role Name** The name of a role in the user recertification. **User Recert Role Description** The description of a role. **User Recert Role Status** The status of a role at the end of the recertification. The valid values are `Approved` and `Rejected`. **User Recert Role Recert Id** A unique numeric identifier that is assigned by IBM Security Identity Manager to a role recertification. **User Recert Role DN** An LDAP Distinguished name for a role entity in the recertification.

Table 244. Query items in the `Recertification Audit` namespace (continued)

Query subject	Query items and their description
Account	**Account Name** The name of an account. **Account Service Dn** An LDAP distinguished name for a service that provisions an account. **Account Status** The status of an account. The valid values are `Active` and `Inactive`. **Account Compliance** The details about an account compliance. The valid values are `Unknown`, `Compliant`, `Non Compliant`, and `Disallowed`. **Account Ownership Type** The ownership type of an account. The valid values are `Individual`, `System`, `Device`, and `Vendor`. **Account Last Access Date** The last date when an account was accessed. **Account Container Dn** An LDAP distinguished name for a business unit to which an account belongs.
Account Service	**Service Name** The name of a service to which an account belongs. **Service Dn** An LDAP distinguished name for a service to which an account belongs. **Service Container DN** An LDAP distinguished name for a business unit of a service that is associated to the accounts. **Service Owner DN** An LDAP distinguished name for a user owner of the service. **Service Url** A URL that connects to the managed resource. **Service Type** The service profile type.
Account Owner	**Person Full Name** The full name of a user who owns an account. **Person Last Name** The surname of a user who owns an account. **Person Status** The status of a user who owns an account. **Person DN** An LDAP distinguished name for an account owner. **Person Business Unit DN** An LDAP distinguished name for a business unit that is associated to an account owner. **Person Supervisor** The supervisor of an account owner.

Table 244. Query items in the Recertification Audit namespace (continued)

Query subject	Query items and their description
Account Recert History	**Recert History Service Name** The name of a service to which accounts and groups belong. These accounts and groups are involved with an account recertification audit. **Recert History Service Profile** The profile type of a service. **Recert History Status** An account status at the end of the recertification workflow process. The valid values are Abort, Approved, Timeout, Pending, and Rejected. **Recert History Action** The action that is taken on an account at the end of recertification process as defined by the recertification policy. The valid values are Abort, Certify, Delete, Mark, Certify Administrative, and Suspend. **Recert History Comments** The comments that are entered by a user during recertification process. **Recert History Process Start Time** The time at which an account recertification workflow process started. **Recert History Process Submission Time** The time at which recertification policy was submitted. **Recert History Process Completion Time** The time at which an account recertification workflow process completed. **Recert History Process Last Modified Time** The last modified time for an account recertification workflow process. **Recert History Process Comments** The comments that are entered by a user during recertification process. **Recert History Process Result Summary** The summary of the recertification process result. The valid values are Success, Failed, Pending, Escalated, Skipped, Timeout, and Warning. **Recert History Process Requestee Name** The name of a user entity for whom the recertification request is submitted. For example, if the entity for recertification is an account, then the query item is the name of the account. **Recert History Process Requester Name** The name of a user who submitted the recertification request. For example, if administrator submits a request for recertification, then this query item is the name of the administrator. **Recert History Recertifier Name** The name of a user who is the final approver in the recertification workflow process. **Recert History Activity Owner** An owner of recertification activity for an account. **Recert History Recertifier Id** An account identifier of the recertifier.

Table 244. Query items in the `Recertification Audit` namespace (continued)

Query subject	Query items and their description
Access	**Group ID** An identifier for a group. **Group Name** The name of a group for which an access is defined. **Group Type** The profile type of a group. **Group Access Name** The name of the access that is defined for a group. **Group Access Type** The type of the access that is defined for a group. **Group DN** An LDAP distinguished name for a group entity for which an access is defined. **Group Container DN** An LDAP distinguished name for a business unit that is associated with a group. **Group Service DN** An LDAP distinguished name for the service that is associated to a group.

Table 244. Query items in the `Recertification Audit` namespace (continued)

Query subject	Query items and their description
Access Recert History	**Recert History Service Name** The name of a service to which accesses and groups belong. These accesses and groups are involved with an access recertification audit. **Recert History Service Profile** The profile type of a service. **Recert History Status** An access status at the end of the recertification workflow process. The valid values are `Abort`, `Approved`, `Timeout`, `Pending`, and `Rejected`. **Recert History Action** The action that is taken on an access at the end of recertification process as defined by the recertification policy. The valid values are `Abort`, `Certify`, `Delete`, `Mark`, `Certify Administrative`, and `Suspend`. **Recert History Comments** The comments that are entered by a user during recertification process. **Recert History Process Start Time** The time at which an access recertification workflow process started. **Recert History Process Submission Time** The time at which recertification policy was submitted. **Recert History Process Completion Time** The time at which an access recertification workflow process completed. **Recert History Process Last Modified Time** The last modified time for an access recertification workflow process. **Recert History Process Comments** The comments that are entered by a user during recertification process. **Recert History Process Result Summary** The summary of the recertification process result. The valid values are `Success`, `Failed`, `Pending`, `Escalated`, `Skipped`, `Timeout`, and `Warning`. **Recert History Process Requestee Name** The name of a user entity for whom the recertification request is submitted. For example, if the entity for recertification is an access, then the query item is the name of the access. **Recert History Process Requester Name** The name of a user who submitted the recertification request. For example, if administrator submits a request for recertification, then this query item is the name of the administrator. **Recert History Recertifier Name** The name of a user who is the final approver in the recertification workflow process. **Recert History Activity Owner** An owner of recertification activity for an access. **Recert History Recertifier Id** An access identifier of the recertifier.

Recertification Config namespace

The Recertification Config namespace provides information about the defined recertification policies and target that is defined for those policies.

Query subjects for Recertification Config namespace

The following table lists the query subjects in the Recertification Config namespace.

Table 245. Query subjects in the Recertification Config namespace

Query subject	Description
Recertification Policy	Represents the recertification policy and its components.
Recertification Policy Schedule	Represents the schedule that is used to auto trigger the recertification policy.
Policy Recertifier	Represents a user who is a recertifier for the recertification policy.
Recert Policy Business Unit	Represents a business unit to which the recertification policy applies.
Recert Policy Role Target	Represents the roles that are recertified by the recertification policy. You must use this query subject with the Recertification Policy to obtain information about the roles that are certified and their configuration attributes.
Recert Policy Access Target	Represents a group access and group membership that are recertified by the recertification policy. You must use this query subject with the Recertification Policy to obtain information about: • Group access • Group membership • Configuration attributes of group access and group membership • Informative attributes of a service that are associated with a group
Recert Policy Access Owner	Represents a group access owner that are recertified by the recertification policy. You must use this query subject with the Recertification Policy to obtain information about the group access owner name.
Group Members	Represents the information about the members of a recertified group. You must use this query subject with the Recert Policy Access Target to obtain information about the members of the recertified group.
Recert Policy Account Target	Represents a service on which the accounts are provisioned and recertified by the recertification policy. You must use this query subject with the Recertification Policy to obtain more information about: • Account recertified • Service on which these accounts are provisioned
Account	Represents account entity and some of its configuration attributes. You must use this query subject with the Recert Policy Account Target to obtain more information about the accounts that are associated with the service.
Person	Represents a user entity and some of its configuration attributes. You must use this query subject with the Recert Policy Role Target query subject to obtain more information about the members of the role.
Account Owner	Represents a user owner of an account. You must use this query subject with the Account query subject to obtain information about the owners of the accounts.

Query items for Recertification Config namespace

The following table lists the query items in the Recertification Config namespace.

Table 246. List of query items in the `Recertification Config` namespace

Query subject	Query items and their description
Recertification Policy	**Recertification Policy Name** The name of the recertification policy. **Recertification Policy Type** The type of an entity that gets recertified by using this policy. The valid values are `User`, `Account`, and `Access`. **Recertification Policy Description** The policy description as specified in the policy configuration. **Recertification Policy Enabled** Shows whether the policy is enabled or not. **Recertification Policy Scheduled** The recertification scheduling modes. The valid values are `CALENDAR` and `ROLLING`. **Recertification Policy Rolling Interval in Days** The recertification period if the recertification policy scheduling mode is `ROLLING`. No value in this query item indicates that the scheduling is not in the `ROLLING` mode. **Recertification Policy Reject Action** An action that is taken if the recertification is rejected. **Recertification Policy Timeout Period in Days** The duration during which a recertifier must act. **Recertification Policy Timeout Action** An automatic action that must be taken if the recertification times out. **Recertification Policy DN** An LDAP distinguished name for the recertification policy. **Recertification Policy Container DN** An LDAP distinguished name for a business unit to which the recertification policy applies. **Recertification Policy Is Custom** Represents whether the recertification policy is customized. It is defined in the workflow. **Recertification Policy User Class** The type of a user to which the recertification policy applies. The valid values are `All`, `Person`, and `Business Partner Person`. **Recertification Policy Scope** Indicates whether the recertification policy applies to the business unit and its subunits or either of them.

Table 246. List of query items in the `Recertification Config` namespace (continued)

Query subject	Query items and their description
Recertification Policy Schedule	**Recertification Policy Detailed Schedule** The recertification schedule in terms of the units of time. **Note:** Do not use this query item with Oracle database. This query item is supported only for DB2 database. **Recertification Policy Schedule** The schedule that automatically triggers the recertification policy. The query item represents the schedule in the numeric format. The format of the schedule is `Minute Hours Month DayOfWeek DayOfMonth DayOfQuarter DayOfSemiAnnual`. For example, `0 0 0 0 -1 0 0`. • `Minute` - Represents the time in minutes. • `Hours` - Represents the time in hours. **-1** indicates that the recertification policy is applied every hour. • `Month` - Represents the month for the recertification. **1** represents `January`, **2** represents `February`, and so on. **-1** indicates that the recertification policy is applied every month. • `DayOfWeek` - Represents the day of a week. **1** represents `Sunday`, **2** represents `Monday`, and so on. The positive value indicates that policy is applied weekly on a specific day. **-1** indicates that the recertification policy is not applied based on the day of a week. • `DayOfMonth` - Represents the date. **-1** indicates that the recertification policy is applied daily. • `DayOfQuarter` - Represents the number of days after the start of each quarter. **0** indicates that the policy is not applied quarterly. • `DayOfSemiAnnual` - Represents the number of days after the start of each half year. **0** indicates that the policy is not applied semi-annually. • The policy is applied annually if the value of `Month` and `DayOfMonth` is positive. **Recertification Policy DN** An LDAP distinguished name for the recertification policy.
Policy Recertifier	**Recertifier Type** The type of the recertifier. The valid values and their meanings: • Account Owner: User being recertified **Note:** This meaning applies only for the recertification policies that are related to the users. For all other recertification policies, `Account Owner` is an owner of the account. • System Administrator: Administrator • Manager: Manager • Person: Specified user • Role: Specified organizational role • System Role: Specified group **Recertifier Name** The name of a specific user, role, or group that is defined as an approver of the recertification. When the recertification policy's recertifier is set to `User being recertified`, then the **Recertifier Name** is shown as a blank. **Recert Policy Dn** An LDAP distinguished name for the recertification policy.

Table 246. List of query items in the `Recertification Config` namespace (continued)

Query subject	Query items and their description
Recert Policy Business Unit	**Business Unit Name** The name of a business unit. **Business Unit Supervisor** The user supervisor of a business unit. **Business Unit Dn** An LDAP distinguished name for a business unit. **Business Unit Container DN** An LDAP distinguished name for the parent organization of a business unit entity.
Recert Policy Role Target	**Role Name** The name of the role. If the policy applies to all the roles in a business unit, then `ALL ROLES WITHIN POLICY ORGANIZATION` is displayed. **Role Description** The description of a role. **Role Type** The type of a role. The valid values are `Static` and `Dynamic`. The value of a role type is empty if the role name is mentioned as `ALL ROLES WITHIN POLICY ORGANIZATION`. **Role Business Unit Name** The business unit to which the role belongs. **Role Business Unit Supervisor** The user supervisor of a business unit to which the role belongs. **Role DN** An LDAP distinguished name for the role. **Role Business Unit DN** An LDAP distinguished name for the business unit to which role belongs. **Recert Policy Dn** An LDAP distinguished name for the recertification policy.

Table 246. List of query items in the `Recertification Config` namespace (continued)

Query subject	Query items and their description
Recert Policy Access Target	**Group Name** The name for a group. If the policy applies to all the groups in an organization, then `ALL GROUPS WITHIN POLICY ORGANIZATION` is displayed. If the policy applies to all the groups for a service, then `ALL GROUPS ON A SPECIFIED SERVICE` is displayed. **Group Description** The description of a group. **Group Type** The profile type of a group. **Group Access Name** An access name that is defined for a group entity. **Group Access Description** The description of an access that is defined for a group entity. **Group Access Type** The type of an access that is defined for a group entity. **Group Service Name** The name of a service on which the group is provisioned. **Group Dn** An LDAP distinguished name for a group. **Group Service DN** An LDAP distinguished name for the service on which a group is provisioned. **Group Container DN** An LDAP distinguished name for an organization to which a group belongs. **Group Service Container Dn** An LDAP distinguished name for an organization of the service on which group is provisioned. **Recert Policy DN** An LDAP distinguished name for the recertification policy.
Recert Policy Access Owner	**Group Dn** An LDAP distinguished name for a group. **Group Access Owner Dn** An LDAP distinguished name for an access owner that is defined for a group entity. **Group Access Owner Full Name** Full name of an access owner that is defined for a group entity.

Table 246. List of query items in the `Recertification Config` namespace (continued)

Query subject	Query items and their description
Group Members	**Account Name** The name of an account that is associated with a credential. **Account Service Dn** An LDAP distinguished name for a service that provisions an account. **Account Status** The status of an account that indicates whether the account is active or inactive. **Account Compliance** The details about an account compliance. The valid values are `Unknown`, `Compliant`, `Non Compliant`, and `Disallowed`. **Account Ownership Type** The ownership type of the account. The valid values are `Individual`, `System`, `Device`, and `Vendor`. **Account Last Access Date** The last accessed date and time of an account. **Account Container Dn** An LDAP distinguished name for a business unit of an account.
Recert Policy Account Target	**Account Service Name** The name of the service. If the policy applies to all the accounts in the service, then `ALL ACCOUNT WITHIN POLICY ORGANIZATION` is displayed. **Account Service Business Unit Name** The name of the business unit to which a service belongs. **Account Service Business Unit Supervisor** A user supervisor of a business unit that is associated with the service. **Account Service DN** An LDAP distinguished name for the service. **Account Service Description** The description of a service. **Account Service Business Unit DN** An LDAP distinguished name for a business unit that is associated with the service. **Account Service Type** The profile type of the service. **Account Service Owner DN** An LDAP distinguished name for an owner of the service. **Account Service Url** A URL that connects to the service. **Recert Policy DN** An LDAP distinguished name for the recertification policy.

Table 246. List of query items in the `Recertification Config` namespace (continued)

Query subject	Query items and their description
Account	**Account Name** The name of an account that is associated with a credential. **Account Service Dn** An LDAP distinguished name for a service that provisions an account. **Account Status** The status of an account that indicates whether the account is active or inactive. **Account Compliance** The details about an account compliance. The valid values are `Unknown`, `Compliant`, `Non Compliant`, and `Disallowed`. **Account Ownership Type** The ownership type of the account. The valid values are `Individual`, `System`, `Device`, and `Vendor`. **Account Last Access Date** The last accessed date and time of an account. **Account Container Dn** An LDAP distinguished name for a business unit of an account.
Person	**Person Full Name** The full name of a user. **Person Last Name** The surname of a user. **Person Status** The status of a user. **Person Dn** An LDAP distinguished name for a user entity. **Person Business Unit Dn** An LDAP distinguished name for a business unit to a user entity. **Person Supervisor** The name of a user for the supervisor of a user entity.
Account Owner	**Person Full Name** The full name of a user who owns an account. **Person Last Name** The surname of a user who owns an account. **Person Status** The status of a user. **Person Dn** An LDAP distinguished name for a user entity. **Person Business Unit Dn** An LDAP distinguished name for a business unit to a user entity. **Person Supervisor** The name of a user for the supervisor of a user entity.

Account Audit namespace

The Account Audit namespace pertains to the audit history of the accounts. This namespace contains query subjects that are related to the audit of accounts, reconciliation, and provisioning policy.

Query subjects for Account Audit namespace

The following table lists the query subjects in the Account Audit namespace.

Table 247. Query subjects in the Account Audit namespace

Query subject	Description
Account Audit	Represents the audit history for the account entities.
Account	Represents an account entity on which the audit actions are performed. This query subject contains configuration and other attributes that represent the status of the account. You must use this query subject with the Account Audit, Reconciliation Audit, and Provisioning Policy to obtain information about the accounts audit actions and provisioning operations.
Reconciliation Audit	Represents the audit history that is associated with the reconciliation operations.
Provisioning Policy	Represents the provisioning policies and their configuration attributes.

Query items for `Account Audit` namespace

The following table lists the query items in the `Account Audit` namespace.

Table 248. Query items in the `Account Audit` namespace

Query subject	Query items and their description
Account Audit	**Audit Account Name** The name of an account on which the audit action is performed. **Audit Action** The action that is performed on an account. For example, `Add`, `Delete`, `Modify`, and `ChangePassword`. **Audit Comments** The comments that are entered by the audit workflow approver. **Audit Account Business Unit** The business unit of an account. **Audit Process Subject** A user who is the owner of an account on which the audit action is performed. **Audit Process Service Profile** The profile type of a service to which an account belongs. **Audit Process Subject Service** The service on which an account is provisioned. **Audit Initiator Name** The name of a user who initiated the audit action. **Audit Process Requestee Name** The name of an account owner. **Audit Process Recertifier Name** The name of a user who approves the audit process workflow. **Audit Operation Start Time** The audit operation initiation date and time. **Audit Activity Owner** An owner who owns the activity. For example, `An owner name who approves the add request for the pending account`. **Audit Activity Name** The name of the audit activity. **Audit Activity Start Time** The audit activity start date and time. **Audit Activity Completion Time** The audit activity completion date and time. **Audit Process Submission Time** The audit process submission date and time. **Audit Process Schedule Time** The date and time at which an event is scheduled for execution. **Audit Process Completion Time** The audit process completion date and time. **Audit Activity Result Summary** The result of the activity within the account audit process. **Audit Process Result Summary** The result of the account audit process.

Table 248. Query items in the `Account Audit` namespace (continued)

Query subject	Query items and their description
Account	**Account Name** The name of an account on which the audit action is performed. **Account Service Name** The name of a service on which the account is provisioned. **Account Status** The account status. The valid values are `Active` and `Inactive`. **Account Is Orphan** Indicates whether an account is associated with a user or not. The valid values are `Yes` and `No`. `Yes` represents the account is orphaned, and `No` represents the account is not orphaned. **Account Compliance** Indicates whether an account is compliant or not. The valid values are `Compliant`, `Non compliant`, `Unknown`, and `Disallowed`. **Account Last Access Date** The last accessed date and time of an account. **Account Owner First Name** The given name of a user who is the owner of an account. **Account Owner Last Name** The surname of a user who is the owner of an account. **Account Dn** An LDAP distinguished name for an account. **Account Service DN** An LDAP distinguished name for the service to which an account belongs. **Account Owner Business Unit Dn** An LDAP distinguished name for the business unit to which an account owner belongs. **Account Owner Dn** An LDAP distinguished name for the account owner.

Table 248. Query items in the `Account Audit` namespace (continued)

Query subject	Query items and their description
Reconciliation Audit	**Reconciliation User Name** The name of a user to whom an account is associated during the reconciliation operation. **Reconciliation Account Name** The name of the reconciled account. **Reconciliation Processed Accounts** The number of processed accounts that exist during the last run of reconciliation. **Reconciliation TIM User Accounts** The number of processed accounts that belong to IBM Security Identity Manager users. **Reconciliation Local Accounts** The total number of local accounts created. It does not include the newly created orphan accounts. **Reconciliation Policy Violations** The number of policy violations that are found for the accounts during the reconciliation. This number includes: • The accounts where an attribute value is different from the local account. • Any attribute value of the account is not compliant with the governing provisioning policies. It does not include the accounts where the attribute values of the local and remote accounts are same, even if the values are noncompliant. **Reconciliation Start Time** The reconciliation operation initiation date and time. **Reconciliation Completion Time** The reconciliation operation completion date and time. **Reconciliation Policy Compliance Status** The reconciliation completion status. **Reconciliation Operation** The operation that is performed for the entry of the service instance. The possible values for an account entry are `New Local`, `New Orphan`, `Suspended Account`, and `Deprovisioned Account`. **Reconciliation Requester Name** The name of an initiator who initiates the reconciliation operation on the account for a service.

Table 248. Query items in the Account Audit namespace (continued)

Query subject	Query items and their description
Provisioning Policy	**Provisioning Policy Name** The name of a provisioning policy through which an account is provisioned on the service. **Provisioning Policy Dn** An LDAP distinguished name for the provisioning policy. **Provisioning Policy Container Dn** An LDAP distinguished name for the business unit to which the provisioning policy applies. **Provisioning Policy Service Name** The name of a service to which the provisioning policy applies. **Provisioning Policy Service Type** The profile type of a service to which the provisioning policy applies. **Provisioning Policy Service Business Unit Name** The business unit of a service to which the provisioning policy applies.

Account Configuration namespace

The Account Configuration namespace contains the query subjects and query items for configuring the accounts.

Query subjects for Account Configuration namespace

The following table lists the query subjects in the Account Configuration namespace.

Table 249. Query subjects in the Account Configuration namespace

Query subject	Description
Account	Represents an account entity and its configuration attributes. The query subject also contains the detailed information about the service to which the account belongs.
Account Owner	Represents a user who owns an account. You must use this query subject with the Account query subject to obtain information about the accounts that are managed by the user.
Account Owner Role Membership	Represents the role information. You must use this query subject with the Account Owner query subject to obtain information about the role membership of the account owners.
Group	Represents the group access and some of its configuration attributes. You must use this query subject with the Account query subject to obtain information about the account members of a group.
Service Business Unit	Represents the business unit to which a service belongs. You must use this query subject with the Account query subject to obtain information about the business unit where the service is located.
Credential	Represents a credential for an account. You must use this query subject with the Account query subject to obtain information about the credential and its configuration attributes.
Credential Pool	Represents a pool of credentials for an account. You must use this query subject with the Account query subject to obtain information about the credential pool and its configuration attributes.
Account ACI	Represents the Access Control Item (ACI) that are applicable on the accounts. You must use this query subject with the Account query subject to obtain information about the accounts that are managed by an ACI.

Table 249. Query subjects in the `Account Configuration` namespace (continued)

Query subject	Description
ACI Operations	Represents the operations that are governed by an ACI. You must use this query subject with the `Account ACI` query subject to obtain information about an ACI associated with the account.
ACI Attribute Permisions	Represents the attributes and operations that can be performed on an attribute. You must use this query subject with the `Account ACI` query subject to obtain information about an ACI associated with the account.
Identity Policy	Represents the identity policy and its configuration attributes. You must use this query subject with the `Account` query subject to obtain information about the accounts that are managed by the policy.
Provisioning Policy	Represents the provisioning policy and some of its configuration attributes. You must use this query subject with the `Account` query subject to obtain information about the policy that provisioned the account.
Recertification Policy	Represents the recertification policy and some of its configuration attributes. You must use this query subject with the `Account` query subject to obtain information about the accounts that are recertified by the policy.
Password Policy	Represents the password policy and its configuration attributes. You must use this query subject with the `Account` query subject to obtain information about the accounts that are managed by the policy.

Query items for Account Configuration namespace

The following table lists the query items in the Account Configuration namespace.

Table 250. Query items in the Account Configuration namespace

Query subject	Query items and their description
Account	**Account Name** The name of an account. **Account Status** An account status. The valid values are Active and Inactive. **Account Compliance** Indicates whether an account is compliant or not. The valid values are Unknown, Compliant, Non Compliant, and Disallowed. **Account Ownership Type** The type of the account ownership. The valid values are Device, Individual, System, and Vendor. **Account Last Access Date** The last accessed date and time of an account. **Account Service Name** The name of a service in which the account is located. **Account Dn** An LDAP distinguished name for an account. **Account Container Dn** An LDAP distinguished name for a business unit to which an account belongs. **Account Service Dn** An LDAP distinguished name for a service to which the accounts belong. **Account Service Container DN** An LDAP distinguished name for a business unit of a service that is associated with the accounts. **Account Service Url** A URL that connects to a managed resource. **Account Service Type** The service profile type.
Account Owner	**Person Full Name** The full name of a user who owns an account. **Person Last Name** The surname of a user who owns an account. **Person Dn** An LDAP distinguished name for an account owner. **Person Business Unit Dn** An LDAP distinguished name for the business unit to which an account owner belongs. **Person Supervisor** The user supervisor of the account owner.

Table 250. Query items in the `Account Configuration` namespace (continued)

Query subject	Query items and their description
Account Owner Role Membership	**Role Name** The name of a role. **Role Type** The type of a role. The valid values are `Static` and `Dynamic`. **Role Dn** An LDAP distinguished name for a role. **Role Container DN** An LDAP distinguished name for the business unit that is associated with a role.
Group	**Group Name** The name of a group for which an access is defined. **Group Type** The profile type of a group. **Group Access Name** The name of the access that is defined for a group. **Group Access Type** The type of the access that is defined for a group. **Group Supervisor** An LDAP distinguished name for a group supervisor. **Group DN** An LDAP distinguished name for a group to which an access is defined. **Group Container Dn** An LDAP distinguished name for the business unit that is associated with a group. **Group Service Dn** An LDAP distinguished name for the service that is associated with a group.
Service Business Unit	**Business Unit Name** The name of the business unit to which a user belongs. **Business Unit Supervisor** The user supervisor of the business unit. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs. **Business Unit Container Dn** An LDAP distinguished name for the parent the business unit of an organization entity.

Table 250. Query items in the `Account Configuration` namespace (continued)

Query subject	Query items and their description
Credential	**Credential Name** The name of a shared credential. **Credential Policy Name** The name of a policy that provides the entitlements for a credential. **Credential Description** Describes a credential as specified in the credential configuration. **Credential Is Exclusive** Indicates whether the credential is exclusive or not. **0** represents `Yes`, and **1** represents `No`. **Credential Pool Use Global Settings** A flag that indicates whether a credential pool uses the shared access global settings. **0** represents `Uses global settings`, and **1** represents `Does not use gloabl settings`. **Credential Is Searchable** Indicates whether a credential is searchable or not. **0** represents `Can be searched`, and **1** represents `cannot be searched`. **Credential Is Password Viewable** Specifies whether a use can view the password on a credential. **0** represents `password is viewable`, and **1** represents `password is not viewable`. **Credential Reset Password** Indicates whether the password of a credential is regenerated on every check-in action. **0** represents `Yes`, and **1** represents `No`. **Credential MAX Checkout Time** The maximum allowed check-out duration for the credential in hours. **Credential Service Name** The name of a service to which the credential is provisioned. **Credential Service Business Unit Name** The name of the business unit to which the credential service belongs. **Credential Dn** An LDAP distinguished name for a credential. **Credential Service Dn** An LDAP distinguished name for the service on which a credential is provisioned. **Credential Service Business Unit Dn** An LDAP distinguished name for the business unit of a credential service. **Credential Shared Access Member Role Dn** An LDAP distinguished name for the role who is a member of the shared access policy that provides entitlement for the credential. **Credential Shared Access Policy Id** a unique numeric identifier that is assigned to the policy by IBM Security Identity Manager.

Table 250. Query items in the `Account Configuration` namespace (continued)

Query subject	Query items and their description
Credential Pool	**Credential Pool Name** The name of the credential pool. **Credential Pool Policy Name** The name of a policy that provides the entitlements for the credential pool. **Credential Pool Service Name** The name of the service on which the groups corresponding to the credential pool are provisioned. **Credential Pool Service Business Unit Name** The name of the business unit to which the credential pool service belongs. **Credential Pool Group Name** The name of the group corresponding to credential pool. **Credential Pool Dn** An LDAP distinguished name for the credential pool. **Credential Pool Service Dn** An LDAP distinguished name for the service on which the groups corresponding to the credential pool are provisioned. **Credential Pool Business Unit Dn** An LDAP distinguished name for the business unit of a credential pool service. **Credential Pool Shared Access Member Role Dn** An LDAP distinguished name for the role who is a member of the shared access policy that provides entitlement for the credential pool. **Credential Pool Shared Access Policy Id** A unique numeric identifier that is assigned to the policy by IBM Security Identity Manager system.

Table 250. Query items in the `Account Configuration` namespace (continued)

Query subject	Query items and their description
Account ACI	**ACI Name** The name of an ACI. **ACI Business Unit Name** The name of a business unit to which an ACI applies. **ACI Protection Category** The category of an entity that is protected by an ACI. The value of this item must be `Account`. **ACI Target** The type of selected protection category that is associated with an ACI. The valid values and their meanings: • `erAccountItem` - All type of the accounts. • `erLDAPUserAccount` - LDAP accounts. • `erPosixAixAccount` - POSIX AIX accounts. • `erPosixHpuxAccount` - POSIX HP-UX accounts. • `erPosixLinuxAccount` - POSIX Linux accounts. • `erPosixSolarisAccount` - POSIX Solaris accounts. **ACI scope** The scope of an ACI. It determines whether an ACI applies to subunits of a business organization or not. The valid values and their meanings: • `single` - The policy applies to a business unit and not its subunits. • `subtree` - The policy applies to the subunits of a business organization. **ACI Member Name** The members who are governed by an ACI. The valid values are: • `All users in the system.` • `The account owner.` • `The manager of the account owner.` • `The owner of the service that the account resides on.` • `The owner of any access defined on the service that the account resides on.` • `The sponsor of the business partner organization in which the account resides.` • `The administrator of the domain in which the account resides.` **ACI System Group Name** Represents the name of the group whose members are governed by an ACI. **ACI Business Unit Dn** An LDAP distinguished name for the business unit. **ACI System Group Dn** An LDAP distinguished name for a system group.
ACI Operations	**ACI Operation Name** The name of an operation that is governed by an ACI. **ACI Operation Permission** The permission applicable on an ACI operation. The valid values are `grant`, `deny`, and `none`. **ACI Business Unit Dn** An LDAP distinguished name for the business unit.

Table 250. Query items in the `Account Configuration` namespace (continued)

Query subject	Query items and their description
ACI Attribute Permisions	**ACI Attribute Name** The name of an LDAP attribute on which the permissions are controlled by an ACI. **ACI Attribute Operation** The name of the operation that can be run on an attribute. The valid values are `r` for read operation, `w` for write operation, and `rw` for read and write operations. **ACI Attribute Permission** The permission applicable on an ACI operation. The valid values are `grant` and `deny`. **ACI Business Unit Dn** An LDAP distinguished name for the business unit.
Identity Policy	**Identity Policy Name** The name of an identity policy. **Identity Policy Scope** The scope of an identity policy. It determines whether the policy applies to the subunits of a business organization or not. The valid values and their meanings: • `single` - The policy applies to a business unit and not its subunits. • `subtree` - The policy applies to the subunits of a business organization. **Identity Policy Enabled** Shows whether or not the policy is enabled. **Identity Policy User Class** The type of a user for which the policy applies. The valid values are `Person` and `Business Partner Person`. **Identity Policy Target Type** Determines the type of the service within the policy business unit on which the identity policy is applied. The valid values and their meanings: • `All Services` - All the defined services. • `Specific Service` - The services that are explicitly added by a user. • `PosixLinuxProfile` - All the services of type POSIX Linux profile. • `LdapProfile` - All the services of type LDAP profile. • `PosixAixProfile` - All the services of type POSIX AIX profile. • `PosixSolarisProfile` - All the services of type POSIX Solaris profile. • `PosixHpuxProfile` - All the services of type POSIX HP_UX Profile. • `ITIM Service` - Default service that is used for IBM Security Identity Manager accounts. **Identity Policy Dn** An LDAP distinguished name for the identity policy. **Identity Policy Target Dn** An LDAP distinguished name for the service on which the identity policy is applied. **Identity Policy Container Dn** An LDAP distinguished name for the business unit where the identity policy is located.

Table 250. Query items in the `Account Configuration` namespace (continued)

Query subject	Query items and their description
Provisioning Policy	**Provisioning Policy Name** The name of a provisioning policy. **Provisioning Policy Member Name** The name of the entities that is provisioned by a policy. The valid values are: • `All users in the organization` • `All other users who are not granted to the entitlement(s) defined by this provisioning policy via other policies.` **Provisioning Policy Dn** An LDAP distinguished name for the provisioning policy. **Provisioning Policy Container Dn** An LDAP distinguished name for a business unit to which the provisioning policy applies.
Recertification Policy	**Recertification Policy Name** The name of the recertification policy. **Recertification Policy Type** The type of an entity that gets recertified by the policy. The valid values are `Account`, `Access`, and `Identity`. **Recertification Policy Description** Describes the policy as specified in the policy configuration. **Recertification Policy Enabled** Shows whether or not the policy is enabled. **Recertification Policy Scheduling Mode** The recertification scheduling modes. The valid values are `CALENDAR` and `ROLLING`. **Recertification Policy Rolling Interval** The recertification period if the recertification policy scheduling mode is `ROLLING`. No value in this query item indicates that the scheduling is not in the `ROLLING` mode. **Recertification Policy Reject Action** An action that is taken if the recertification is rejected. **Recertification Policy Timeout Period in Days** The duration during which the recertifier must act. **Recertification Policy Timeout Action** An automatic action that must be taken if the recertification times out. **Recertification Policy DN** An LDAP distinguished name for the recertification policy. **Recertification Policy Container DN** An LDAP distinguished name for a business unit to which the recertification policy applies. **Recertification Policy IsCustom** Indicates whether this recertification policy is customized. It is defined in a workflow. **Recertification Policy User Class** The type of a user the recertification policy applies. The valid values are `All`, `Person`, and `Business Partner Person`.

Table 250. Query items in the `Account Configuration` namespace (continued)

Query subject	Query items and their description
Password Policy	**Password Policy Name** The name of a password policy. **Password Policy Scope** The scope of a password policy. It determines whether the policy applies to subunits of a business organization or not. The valid values and their meanings: • `single` - The policy applies to a business unit and not its subunits. • `subtree` - The policy applies to the subunits of a business organization. **Password Policy Enabled** Shows whether or not the policy is enabled. **Password Policy Target Type** Determines the type of a service within the policy business unit on which the password policy is applied. The valid values are: • `All Services` - All the defined services. • `Specific Service` - The services that are explicitly added by a user. • `PosixLinuxProfile` - All the services of type POSIX Linux profile. • `LdapProfile` - All the services of type LDAP profile. • `PosixAixProfile` - All the services of type POSIX AIX profile. • `PosixSolarisProfile` - All the services of type POSIX Solaris profile. • `PosixHpuxProfile` - All the services of type POSIX HP_UX Profile. • `ITIMService` - Default service that is used for IBM Security Identity Manager accounts. **Password Policy Dn** An LDAP distinguished name for the password policy. **Password Policy Target Dn** An LDAP distinguished name for the service on which the password policy is applied. **Password Policy Container Dn** An LDAP distinguished name for the business unit where the identity policy is located.

`Provisioning Policy Audit` namespace

The `Provisioning Policy Audit` namespace pertains to the audit history of the provisioning policies. You can generate the audit reports for the actions that are performed on the provisioning policies and automatically provisioned accounts.

Query subjects for `Provisioning Policy Audit` namespace

The following table lists the query subjects in the `Provisioning Policy Audit` namespace.

Table 251. Query subjects in the `Provisioning Policy Audit` namespace

Query subject	Description
Provisioning Policy Audit	Represents a history of the provisioning policies and accounts.

Table 251. Query subjects in the `Provisioning Policy Audit` namespace (continued)

Query subject	Description
Provisioning Policy	Represents the provisioning policies on which the audit actions are performed. To obtain more information about the policy and accounts that go through the audit actions, use this query subject with the following query subjects: • `Provisioning Policy Audit` • `Provisioning Policy Business Unit` • `Provisioning Policy Service`
Provisioning Policy Business Unit	Represents the business unit to which the provisioning policy applies.
Provisioning Policy Service	Represents the managed service to which the provisioning policy applies.

Query items for `Provisioning Policy Audit` namespace

The following table lists the query items in the `Provisioning Policy Audit` namespace.

Table 252. Query items in the `Provisioning Policy Audit` namespace

Query subject	Query items and their description
Provisioning Policy Audit	**Audit Provisioning Policy Name** The name of a provisioning policy. **Audit Provisioning Policy Business Unit** The name of a business unit to which the provisioning policy applies. **Audit Action** The action that is performed on the provisioning policy. For example, `Add`, `Modify`, and `EnforceEntirePolicy`. **Audit Process Subject** A subject of the automatically provisioned audit action. It can be the provisioning policy or the accounts that are provisioned. **Audit Subject Type** The type of the audit subject. For example, `Policy` and `Account`. **Audit Process Subject Profile** The profile type of the accounts that is provisioned by the provisioning policy. This query item applies only to the accounts. **Audit Process Subject Service** The service on which the accounts are provisioned. This query item applies only to the accounts. **Audit Initiator Name** The name of a user who initiated the audit action. **Audit Process Requestee Name** The name of a user on behalf of whom the audit action is initiated. **Audit Comments** The comments that are entered by an approver during the audit workflow approval. **Audit Operation Start Time** The audit operation start date and time. **Audit Process Submission Time** The audit process submission date and time. **Audit Process Schedule Time** The date and time at which an event is scheduled for execution. **Audit Process Completion Time** The audit process completion date and time. **Audit Process Result Summary** The result summary of the account request workflow process. **Activity Name** The name of the audit activity. **Activity Submission Time** The audit activity submission date and time. **Activity Completion Time** The audit activity completion date and time. **Audit Activity Result Summary** The result summary of an activity in the account request workflow process. **Audit Process Recertifier** The name of a user who approves the audit process workflow. **Audit provisioning policy Dn** An LDAP distinguished name for the provisioning policy on which the audit actions are performed.

Table 252. Query items in the Provisioning Policy Audit namespace (continued)

Query subject	Query items and their description
Provisioning Policy	**Provisioning Policy Name** The name of a provisioning policy. **Provisioning Policy Scope** The scope in terms of a hierarchy of the business units to which the provisioning policy applies. **Provisioning Policy Dn** An LDAP distinguished name for the provisioning policy. **Provisioning Policy Business Unit Dn** An LDAP distinguished name for the business unit to which the provisioning policy applies.
Provisioning Policy Business Unit	**Business Unit Name** The name of the business unit to which the provisioning policy applies. **Business Unit Supervisor** The supervisor of a user for the business unit to which the provisioning policy applies. **Business Unit Container Dn** An LDAP distinguished name for the business unit where the provisioning policy business unit is located. **Business Unit Dn** An LDAP distinguished name for the business unit to which the provisioning policy belongs.
Provisioning Policy Service	**Service Name** The name of a service to which the provisioning policy applies. **Service Type** The profile type of a service to which the provisioning policy applies. **Service Business Unit** The business unit of a service to which the provisioning policy applies. **Service Dn** An LDAP distinguished name for a service to which the provisioning policy belongs. **Service Business Unit Dn** An LDAP distinguished name for the business unit to which the service belongs. **Service Owner Dn** An LDAP distinguished name for the user owner of a service.

Provisioning Policy Config namespace

The Provisioning Policy Config namespace pertains to the configuration attributes of a provisioning policy. It encompasses the business units, services, policy members, and the ACIs that are related to the provisioning policies. You can generate the configuration reports for the provisioning policy.

Query subjects for Provisioning Policy Config namespace

The following table lists the query subjects in the Provisioning Policy Config namespace.

Table 253. Query subjects in the `Provisioning Policy Config` namespace

Query subject	Description
Provisioning Policy	Represents the provisioning policy and its configuration attributes.
Provisioning Policy Parameters	Represents the parameters that are defined for the entitlements of a provisioning policy. You must use this query subject with the `Provisioning Policy` query subject.
Provisioning Policy Role Members	Represents the user members of a role that is a part of the provisioning policy. You must use this query subject with the `Provisioning Policy` query Subject.
ACI Attribute Permissions	Represents the permissions that are defined on the attributes by an ACI. You must use this query subject with the `Provisioning Policy ACI` query subject.
ACI Operations	Represents the permissions that are defined on the class operations by an ACI. You must use this query subject with the `Provisioning Policy ACI` query subject.
Provisioning Policy ACI	Represents an ACI associated with a provisioning policy. You must use this query subject with the `Provisioning Policy` query subject.

Query items for `Provisioning Policy Config` namespace

The following table lists the query items in the `Provisioning Policy Config` namespace.

Note: The policies that are in the `Draft` mode cannot be identified. Although the draft policies are in the list, there is no attribute that can identify the draft policies.

Table 254. Query items in the `Provisioning Policy Config` namespace

Query subject	Query items and their description
Provisioning Policy	**Provisioning Policy Name** The name of a provisioning policy. **Provisioning Policy Business Unit** The name of a business unit to which the provisioning policy applies. **Provisioning Policy Is Enabled** Represents whether the provisioning policy is enabled or not. The valid values are `Enabled` and `Disabled`. **Provisioning Policy Priority** An integer number greater than zero that indicates the priority of the provisioning policy. **Provisioning Policy Scope** The scope in terms of a hierarchy of the business units to which the provisioning policy applies. The valid values are `Single` and `Subtree`. **Provisioning Policy Member Name** The name of a role or user who is a member of the provisioning policy. The valid values are `All users in the organization`, `All other users who are not granted to the entitlement(s) defined by this provisioning policy via other policies`, or the names of the roles who are the members. **Provisioning Policy Dn** An LDAP distinguished name for the provisioning policy. **Provisioning Policy Business Unit Dn** An LDAP distinguished name for the business unit to which the provisioning policy applies. **Provisioning Policy Service Name** The name of a service to which the provisioning policy applies. **Provisioning Policy Service Type** The profile type of a service to which the provisioning policy applies. **Provisioning Policy Service Url** A URL of a service to which the provisioning policy applies. **Provisioning Policy Service Business Unit** The business unit of a service to which the provisioning policy applies.
Provisioning Policy Parameters	**Provisioning Policy Parameter** A provisioning policy parameter that is defined by the system administrator. **Provisioning Policy Parameter Value** The parameter value. **Provisioning Policy Parameter Enforcement Type** Specifies the rule for the system to evaluate an attribute value validity. The possible values are `Mandatory`, `Allowed`, `Default`, and `Excluded`. **Service Target** An LDAP distinguished name for the service that is associated with the provisioning policy.

Table 254. Query items in the `Provisioning Policy Config` namespace (continued)

Query subject	Query items and their description
Provisioning Policy Role Members	**Role Member First Name** The given name of a role member. **Role Member Last Name** The surname of a role member. **Role Member Status** The current state of the role member. The valid values are `Active` and `Inactive`. **Role Member Dn** An LDAP distinguished name for a role member. **Role Member Business Unit Dn** An LDAP distinguished name for the business unit of a role member. **Role Member Supervisor** The user supervisor of the role member.
ACI Attribute Permissions	**ACI Attribute Name** The name of an attribute that is controlled by an ACI. **ACI Attribute Operation** The name of an operation that is governed by an ACI. **ACI Attribute Permission** The permission that applies on an ACI operation. The valid values are `grant`, `deny`, and `none`. **ACI Business Unit Dn** An LDAP distinguished name for the business unit.
ACI Operations	**ACI Operation Name** The class operation for an ACI. For example, `Search`, `Add`, and `Modify`. **ACI Operation Permission** The permission that is associated with a class operation. The valid values are `grant`, `deny`, and `none`. **ACI Business Unit Dn** An LDAP distinguished name for the business unit to which an ACI applies.

Table 254. Query items in the `Provisioning Policy Config` namespace (continued)

Query subject	Query items and their description
Provisioning Policy ACI	**ACI Name** The name of an ACI associated with the provisioning policy. **ACI Business Unit** The name of a business unit to which an ACI applies. **ACI Scope** The hierarchy of the business units to which an ACI applies. **ACI Member Name** The members who are governed by an ACI. The valid values are: • `All Users` - All users in the system. • `All Group Members` - The users who are the members of these groups. • `Supervisor` - The supervisor of the business unit in which the provisioning policy resides. • `Sponsor` - The sponsor of the business partner organization in which the role resides. • `Administrator` - The administrator of the domain in which the account resides. **ACI System Group Name** The name for IBM Security Identity Manager group that is the part of an ACI. This query item is valid only when ACI member name is the name of the user members of a specified group. **ACI Business Unit Dn** An LDAP distinguished name for the business unit to which an ACI applies. **ACI Role Dn** An LDAP distinguished name for IBM Security Identity Manager group that is a part of an ACI. **ACI Role Business Unit Dn** An LDAP distinguished name for a business unit that is associated with IBM Security Identity Manager group. **ACI Parent** An LDAP distinguished name for the parent container in which an ACI is defined.

`Role Audit` namespace

The `Role Audit` namespace pertains to the audit history of the actions that are performed on the roles. You can generate the audit reports for the role entities.

Query subjects for `Role Audit` namespace

The following table lists the query subjects in the `Role Audit` namespace.

Table 255. Query subjects in the `Role Audit` namespace

Query subject	Description
Role	Represents the role entity and its configuration attributes on which the audit actions are performed.
Role Audit	Represents the audit history of the role entities. You must use this query subject with the `Role` query subject.
Role Business Unit	Represents the business unit to which a role associated with the audit action belongs. You must use this query subject with the `Role` query subject.

Table 255. Query subjects in the Role Audit namespace (continued)

Query subject	Description
Role Membership	Represents the person who is the member of a role and its configuration attributes. You must use this query subject with the Role query subject.
Role Owner	Represents an owner of a role that is associated with the audit action. The owner can be a user or role. You must use this query subject with the Role query subject.

Query items for Role Audit namespace

The following table lists the query items in the Role Audit namespace.

Table 256. List of query items in the Role Audit namespace

Query subject	Query items and their description
Role	**Role Name** The name of a role on which the audit actions are performed. **Role Description** The description of the role. **Role Type** The type of a role. The valid values are Static and Dynamic. **Role Dn** An LDAP distinguished name for the role. **Role Container Dn** An LDAP distinguished name for the container of the role.

Table 256. List of query items in the `Role Audit` namespace (continued)

Query subject	Query items and their description
Role Audit	**Audit Role Name** The name of a role entity on which the audit action is performed. **Audit Role Business Unit** The business unit of the role. **Audit Action** The action that is performed on a role. For example, `Add`, `Modify`, `Delete`, and `AddMember`. **Audit Comments** The comments that are entered by the audit workflow approver. **Note:** Along with the audit comments, this query item might contain the operational data. **Audit Initiator Name** The name of a user who initiated the audit action. **Audit Process Requestee Name** The name of a user who is added to the role. This query item is applicable only to `AddMember` audit action. **Audit Process Recertifier Name** The name of a user who approved the audit action. **Audit Operation Start Time** The audit operation start date and time. **Audit Process Submission Time** The audit process submission date and time. **Audit Process Schedule Time** The date and time at which an event is scheduled for execution. **Audit Process Completion Time** The audit process completion date and time. **Audit Process Subject** The subject on which the audit action was performed. It applies to the cases where the defined workflow must complete before the audit action completion. **Audit Process Subject Profile** The profile type of an entity that is associated with the audit action. This query item contains the value only if the `Audit Process Subject` contain a value. **Audit Process Subject Service** The service to which an entity represented by the `Audit Process Subject` query item belongs. **Audit Process Result Summary** The result of a role audit process. **Activity Result Summary** The result of an activity within a role audit process. **Audit Activity Name** The name of the activity that corresponds to the audit process. **Audit Activity Owner** An owner who owns the activity. For example: `Approve role membership or Add request.`

Table 256. List of query items in the `Role Audit` namespace (continued)

Query subject	Query items and their description
Role Business Unit	**Business Unit Name** The name of a business unit to which the role belongs. **Business Unit Supervisor** A person who is the supervisor of a business unit to which the role belongs. **Business Unit Dn** An LDAP distinguished name for a business unit to which the role belongs. **Business Unit Container DN** An LDAP distinguished name for the parent organization of the business unit to which the role belongs.
Role Membership	**Role Member First Name** The given name of a role member. **Role Member Last Name** The surname of a role member. **Role Member Supervisor** The supervisor of a role member. **Role Member Dn** An LDAP distinguished name for a role member. **Role Dn** An LDAP distinguished name for a role. **Role Member Business Unit Dn** An LDAP distinguished name for the business unit to which a role member belongs.
Role Owner	**Role Owner Name** The name of an owner of the role. **Role Owner Type** Indicates whether the owner is a role or a user. The valid values are `User` and `Role`. **Role Owner Business Unit** The business unit to which the role owner belongs. **Role Dn** An LDAP distinguished name for a role.

`Role Configuration` namespace

The `Role Configuration` namespace contains the query subjects and query items for configuring the roles.

Query subjects for `Role Configuration` namespace

The following table lists the query subjects in the `Role Configuration` namespace.

Table 257. Query subjects in the `Role Configuration` namespace

Query subject	Description
Role	Represents a role and some of its configuration attributes.
Role Owner	Represents an owner of a role that is associated with the audit action. The owner can be a user or role. You must use this query subject with the `Role` query subject.

Table 257. Query subjects in the `Role Configuration` namespace (continued)

Query subject	Description
Parent Roles	Represents the parent of a role. You must use this query subject with the `Role` query subject to obtain information about the parent of the role.
Role Assignment Attributes	Represents an assignment attributes for a role. You must use this query subject with the `Role` query subject to obtain information about the assignment attributes for the role.
Role Members	Represents the user members of a role. You must use this query subject with the `Role` query subject to obtain information about the members of the role.
Role ACI	Represents an ACI that is applicable on the roles. You must use this query subject with the `Role` query subject to obtain information about the roles that are managed by an ACI.
ACI Operations	Represents information about operations that are governed by an ACI. You must use this query subject with the `Role ACI` query subject to obtain information about an ACI associated with the role.
ACI Attribute Permissions	Represents information about the attributes and operations that can be performed on the attributes. You must use this query subject with the `Role ACI` query subject to obtain information about an ACI associated with a role.
Recertification Policy	Represents the recertification policy and some of its configuration attributes. You must use this query subject with the `Role` query subject to obtain information about the roles that are recertified by the recertification policy.
Recertification Policy Business Unit	Represents a business unit to which the recertification policy is applicable.
Provisioning Policy	Represents the provisioning policy and some of its configuration attributes. You must use this query subject with the `Role` query subject to obtain information about the roles who are member of a provisioning policy.
Shared Access Policy	Represents the shared access policy that provides entitlements for the credentials and credential pools. You must use this query subject with the `Role` query subject to obtain information about the role members of the shared access policy.
Separation of Duty Policy	Represents a separation of duty policy and some of its configuration attributes. You must use this query subject with the `Role` query subject to obtain information about the roles to which the policy applies.
Separation of Duty Rule	Represents the rule that is defined for a separation of duty policy. You must use this query subject with the `Separation of Duty Policy` and `Role` query subjects to obtain information about: • The rules that are defined for a separation of duty policy. • The roles that are covered by a separation of duty rule.

Query items for `Role Configuration` namespace

The following table lists the query items in the `Role Configuration` namespace.

Table 258. List of query items in the `Role Configuration` namespace

Query subject	Query items and their description
Role	**Role Name** The name of a role. **Role Description** The description of a role. **Role Type** The type of a role. The valid values are `Static` and `Dynamic`. **Role Access Enabled** Represents whether an access for a role is enabled or not. True represents `Enabled`, and False represents `Disabled`. **Role Common Access Enabled** Represents whether a common access for the role is enabled or not. The valid values are `True` and `False`. **Role Access Type** The type of an access that is enabled for a role. **Role Business Unit Name** The name of a business unit to which the role belongs. **Role Dn** An LDAP distinguished name for the role. **Role Business Unit Dn** An LDAP distinguished name for the business unit of a role. **Role Business Unit Container Dn** An LDAP distinguished name for the parent organization of the business unit. **Role Business Supervisor** The supervisor of a user for the business unit.
Role Owner	**Role Owner Name** The name of an owner of the role. **Role Owner Type** Indicates whether the owner is a role or a user. The valid values are `User` and `Role`. **Role Owner Business Unit** The business unit to which the role owner belongs. **Role Dn** An LDAP distinguished name for a role.
Parent Roles	**Parent Role Name** The name of the parent role. **Parent Role Dn** An LDAP distinguished name for the role. **Parent Business Unit Dn** An LDAP distinguished name for the business unit of the parent role.
Role Assignment Attributes	**Attribute Name** The name of an attribute. **Role Dn** An LDAP distinguished name for the role to which an attribute is assigned.

Table 258. List of query items in the `Role Configuration` namespace (continued)

Query subject	Query items and their description
Role Members	**Role Member First Name** The given name of a role member. **Role Member Last Name** The surname of a role member. **Role Member Attribute Name** The name of the assignment attribute that is associated with a role member. **Role Member Attribute Value** An assignment attribute value that is associated with a role member. **Role Member Dn** An LDAP distinguished name for a role member. **Role Member Business Unit Dn** An LDAP distinguished name for the business unit of a role member.
Role ACI	**Role ACI Name** The name of an ACI that applies to a role. **Role ACI Protection Category** The type of a role that is protected by an ACI. The valid values are `Static Role` and `Dynamic Role`. **Role ACI Scope** The scope of an ACI. It determines whether an ACI applies to sub units of a business organization or not. The valid values and their meanings: • `single` - The policy applies to a business unit and not its subunits. • `subtree` - The policy applies to the subunits of a business organization. **Role ACI Member Name** The members who are governed by an ACI. The valid values are: • `All users in the system.` • `The supervisor of the business unit in which the role resides.` • `The owners of the role, The administrator of the domain in which the role resides.` • `The sponsor of the business partner organization in which the role resides.` **Role ACI System Group Name** Represents the name of the group whose members are governed by an ACI. **Role ACI Business Unit Dn** An LDAP distinguished name for a business unit. **Role ACI System Group Dn** An LDAP distinguished name for a system group.

Table 258. List of query items in the `Role Configuration` namespace (continued)

Query subject	Query items and their description
ACI Operations	**ACI Operation Name** The name of an operation that is governed by an ACI. **ACI Operation Permission** The permission applicable on an ACI operation. The valid values are `grant`, `deny`, and `none`. **ACI Business Unit Dn** An LDAP distinguished name for the business unit to which an ACI applies.
ACI Attribute Permissions	**ACI Attribute Name** The name of an LDAP attribute on which the permissions are controlled by an ACI. **ACI Attribute Operation** The name of an operation that an ACI governs. **ACI Attribute Permission** The permission applicable on an ACI operation. The valid values are `grant` and `deny`. **ACI Business Unit Dn** An LDAP distinguished name for a business unit to which an ACI applies.

Table 258. List of query items in the `Role Configuration` namespace (continued)

Query subject	Query items and their description
Recertification Policy	**Recertification Policy Name** The name of the recertification policy. **Recertification Policy Type** The type of an entity that gets recertified by using this policy. The valid values are: `Account`, `Access`, and `Identity`. **Recertification Policy Description** Describes the policy as specified in the policy configuration. **Recertification Policy Enabled** Shows whether or not the policy is enabled. **Recertification Policy Scheduling Mode** The recertification scheduling modes. The valid values are `CALENDAR` and `ROLLING`. **Recertification Policy Rolling Interval** Represents the recertification period if the recertification policy scheduling mode is `ROLLING`. No value in this query item indicates that the scheduling is not in the `ROLLING` mode. **Recertification Policy Reject Action** An action that is taken if the recertification is rejected. **Recertification Policy Timeout Period in Days** The duration during which a recertifier must act. **Recertification Policy Timeout Action** The automatic action that must be taken if the recertification times out. **Recertification Policy DN** An LDAP distinguished name for the recertification policy. **Recertification Policy Container DN** An LDAP distinguished name for a business unit to which the recertification policy applies. **Recertification Policy IsCustom** Indicates whether the recertification policy is customized or not. It is defined in the workflow. **Recertification Policy User Class** The type of a user to which the recertification policy applies. The valid values are `All`, `Person`, and `Business Partner Person`.
Recertification Policy Business Unit	**Business Unit Name** The name of a business unit. **Business Unit Supervisor** The user supervisor of a business unit. **Business Unit Dn** An LDAP distinguished name for a business unit. **Business Unit Container DN** an LDAP distinguished name for the parent business unit.

Table 258. List of query items in the `Role Configuration` namespace (continued)

Query subject	Query items and their description
Provisioning Policy	**Provisioning Policy Name** The name of the provisioning policy. **Provisioning Policy Business Unit Name** The name of a business unit to which the provisioning policy applies. **Provisioning Policy Dn** An LDAP distinguished name for the provisioning policy. **Provisioning Policy Business Unit Dn** An LDAP distinguished name for the business unit to which the provisioning policy applies. **Provisioning Policy Business Supervisor** A user supervisor for the provisioning policy business unit.
Shared Access Policy	**Shared Access Policy Name** The name of a shared access policy. **Shared Access Policy Description** The description the shared access policy. **Shared Access Policy Business Unit Name** The name of a business unit to which the shared access policy applies. **Shared Access Policy Scope** The scope of a shared access policy in terms of business units the policy applies. **1** represents that the policy applies to the business unit only, and **2** indicates that the policy applies to the sub business units also. **Shared Access Policy Status** Represents whether a policy is enabled or not. **0** represents `Enabled`, and **1** represents `Disabled`. **Shared Access Business Unit Supervisor** A user supervisor for the shared access policy business unit. **Shared Access Policy ID** A unique numeric identifier that is assigned to the policy by IBM Security Identity Manager. **Shared Access Policy Business Unit Dn** An LDAP distinguished name for the business unit to which a shared access policy applies.

Table 258. List of query items in the Role Configuration namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy	**Separation of Duty Policy Name** The name of the separation of duty policy. **Separation of Duty Policy Description** The description of the separation of duty policy. **Separation of Duty Policy Business Unit Name** The name of the business unit to which the separation of duty policy applies. **Separation of Duty Policy Enabled** Represents whether the policy is enabled or not. **True** represents Enabled, and **False** represents Disabled. **Separation of Duty Policy Owner Name** The name of an owner of the separation of duty policy. **Separation of Duty Policy Owner Type** the type of an owner for the separation of duty policy. The valid values are Role and Person. **Separation of Duty Policy Owner Business Unit Name** The name of the business unit that applies to the policy owner. **Separation of Duty Policy Id** A unique numeric identifier that IBM Security Identity Manager assigns to the policy. **Separation of Duty Policy Owner Dn** An LDAP distinguished name for the policy owner.
Separation of Duty Rule	**Separation of Duty Rule Name** The name of the separation of duty rule. **Separation of Duty Rule Max Roles Allowed** The maximum number of roles that are allowed in a rule. **Separation of Duty Rule Version** A numeric identifier for the current version of the rule that applies to a policy. **Separation of Duty Rule Id** A unique numeric identifier that IBM Security Identity Manager assigns to the rule. **Separation of Duty Policy Id** A unique numeric identifier that IBM Security Identity Manager assigns to the policy. **Separation of Duty Role Id** A unique numeric identifier that IBM Security Identity Manager assigns to the role.

Separation of Duty Audit namespace

The Separation of Duty Audit namespace pertains to the audit history, exemption and violation of the separation of duty policy.

Query subjects for Separation of Duty Audit namespace

The following table lists the query subjects in the Separation of Duty Audit namespace.

Table 259. Query subjects in the Separation of Duty Audit namespace

Query subject	Description
Separation of Duty Policy	Represents the separation of duty policy and the rules that are configured. You must use this query subject with the following query subjects to generate the violation and exemption reports: • Separation of Duty Policy Violation and Exemption History. • Separation of Duty Policy Violation and Exemption Current Status. • Separation of Duty Policy Audit.
Separation of Duty Policy Role	Represents the configuration attributes of a role. The role is a part of the rule that is associated with the separation of duty policy. You must use this query subject with the Separation of Duty Policy query subject.
Separation of Duty Policy Violation and Exemption Current Status	Provides information about the exemption and violation for a separation of duty policy. You must use this query subject with the Separation of Duty Policy query subject.
Separation of Duty Policy Violation and Exemption History	Represents the historical information about exemption and violation for a separation of duty policy. You must use this query subject with the Separation of Duty Policy query subject.
Separation of Duty Policy Audit	Represents the audit history for the separation of duty policy. The actions that are audited in this query subject are Add, Modify, Delete, Reconcile, and Revoke. You must use this query subject with the Separation of Duty Policy query subject to generate an audit history report.
Separation of Duty Policy Role Conflict	Provides information about: • The roles that are involved in a violation. • The role on the person that is found to be in violation of the separation of duty policy rule. You must use this query subject with the Separation of Duty Policy Violation and Exemption Current Status query subject to obtain more information about the violation that is occurred.

Query items for Separation of Duty Audit namespace

The following table lists the query items in the Separation of Duty Audit namespace.

Table 260. Query items in the `Separation of Duty Audit` namespace

Query subject	Query items and their description
Separation of Duty Policy	**Separation of Duty Policy Name** The name of the separation of duty policy. **Separation of Duty Policy Description** The description of the separation of duty policy. **Separation of Duty Policy Business Unit Name** The name of a business unit to which the separation of duty policy applies. **Separation of Duty Policy Enabled** Indicates whether or not the policy is enabled. The valid values are `Enabled` and `Disabled`. **Separation of Duty Policy Rule Name** The name of a rule that is associated with the separation of duty policy. **Separation of Duty Policy Rule Max Roles Allowed** The maximum number of the roles that can be a part of the separation of duty rule. **Separation of Duty Policy Id** A unique numeric identifier for the separation of duty policy. **Separation of Duty Policy Dn** An LDAP distinguished name for the separation of duty policy. **Separation of Duty Rule Id** A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.
Separation of Duty Policy Role	**Separation of Duty Policy Role Name** The name of the role that is a part of the separation of duty rule. **Separation of Duty Policy Role Description** The description of the separation of duty policy role. **Separation of Duty Policy Business Unit Name** The name of the business unit to which the separation of duty policy role applies. **Separation of Duty Policy Role Dn** An LDAP distinguished name for the role that is a part of the separation of duty policy. **Separation of Duty Policy Role Id** A unique numeric identifier for the role that is a part of separation of duty policy. **Separation of Duty Policy Rule Id** A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.

Table 260. Query items in the `Separation of Duty Audit` namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Violation and Exemption Current Status	**Audit Status** The status of the separation of duty policy violation or exemption. The possible values are: • `Violation` - indicates that the violation occurred. • `Approved` - indicates that an approver approved the exempted violation. **Audit Person Name** The name of a person to which the violation refers. **Audit Person Business Unit** The business unit to which a person involved in the violation belongs. **Audit Approver Name** The name of a person who exempted the violation. **Audit Approver Business Unit** The business unit of the user who exempted the violation. **Audit Approver Comment** The comment that is added by an approver during the violation exemption process. **Audit Policy Rule Name** The name of a rule that is associated with the separation of duty policy. **Audit Policy Rule Max Roles Allowed** The maximum number of the roles that can be a part of the separation of duty rule. **Audit Policy Rule Version** The separation of duty rule version. **Audit Time Stamp** The audit action occurrence time stamp. **Audit Exemption Time Stamp** The time stamp of the last violation occurred during separation of duty policy evaluation. **Audit Violation Id** A unique numeric identifier for the violation record. **Audit Policy Global Id** A unique identifier for the separation of duty policy. **Audit Rule Global Id** A unique identifier for the separation of duty policy rule. **Audit Person Global Id** A unique identifier for the person against whom the violation occurred.

Table 260. Query items in the `Separation of Duty Audit` namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Violation and Exemption History	**Audit Status** The status of the separation of duty policy violation or exemption. The possible values are: • `Violation` - indicates that the violation occurred. • `Approved` - indicates that an approver approved the exempted violation. **Audit Person Name** The name of a person to which the violation refers. **Audit Person Business Unit** The business unit to which a person involved in the violation belongs. **Audit Approver Name** The name of a person who exempted the violation. **Audit Approver Business Unit** The business unit of the user who exempted the violation. **Audit Approver Comment** The comment that is added by an approver during the violation exemption process. **Audit Policy Rule Name** The name of a rule that is associated with the separation of duty policy. **Audit Policy Rule Max Roles Allowed** The maximum number of the roles that can be a part of the separation of duty rule. **Audit Policy Rule Version** The separation of duty rule version. **Audit Time Stamp** The audit action occurrence time stamp. **Audit Violation Id** A unique numeric identifier for the violation record. **Audit Policy Global Id** A unique identifier for the separation of duty policy. **Audit Rule Global Id** A unique identifier for the separation of duty policy rule. **Audit Person Global Id** A unique identifier for the person against whom the violation occurred.

Table 260. Query items in the `Separation of Duty Audit` namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Audit	**Audit Separation of Duty Policy Name** The name of the separation of duty policy. **Audit Separation of Duty Policy Business Unit** The business unit of the separation of duty policy. **Audit Action** An action that is performed on the separation of duty policy. For example, `Add`, `Modify`, `Delete`, and `Reconcile`. **Audit Comments** The comments that are entered by the approver. **Audit Process Subject** The name of the separation of duty policy on which the audit action occurs. **Audit Process Subject Profile** The profile type of an entity that is associated with the audit action. This query item contains the value only if the `Audit Process Subject` contains a value. **Audit Process Subject Service** The service to which an entity represented by the `Audit Process Subject` query item belongs. **Audit Process Recertifier Name** The name of a user who approves the audit process workflow. **Audit Process Requestee Name** The entity upon which the audit action is performed. **Audit Initiator Name** The name of a user who initiates the audit action. **Audit Activity Owner** The name of a user who owns the audit activity. **Audit Activity Name** The name of the audit activity. **Audit Operation Start Time** The audit operation initiation date and time. **Audit Process Submission Time** The audit process submission date and time. **Audit Process Schedule Time** The date and time at which an event is scheduled for execution. **Audit Process Completion Time** The audit process completion date and time. **Audit Activity Result Summary** The result of an activity within the account audit process. **Audit Process Result Summary** The result of an account audit process.

Table 260. Query items in the Separation of Duty Audit namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Role Conflict	**User Roles in Conflict** The name of the role on the person that is found in violation of the separation of duty policy rule. **User Roles in Conflict Role Dn** An LDAP distinguished name for a role on the person that is found in violation of the separation of duty policy rule. **User Roles in Conflict Business Unit Dn** An LDAP distinguished name for the business unit of a role on the person that is found in violation of the separation of duty policy rule. **User Roles in Conflict Owner Dn** An LDAP distinguished name for an owner of a role. The referred role is the role that participates in the separation of duty policy. This query item might be empty if no owners are assigned to the role. **Policy Roles in Conflict** The name of the role as referenced in the separation of duty policy rule that is involved in the violation. **Policy Roles in Conflict Role Dn** An LDAP distinguished name for the role as referenced in the separation of duty policy rule that is involved in the violation. **Policy Roles in Conflict Business Unit Dn** An LDAP distinguished name for the business unit of a role as referenced in the separation of duty policy rule that is involved in the violation. **Policy Roles in Conflict Owner Dn** An LDAP distinguished name for an owner of a role. The referred role is the role that associates with a user. This query item might be empty if no owners are assigned to the role. **Separation of Duty Policy Violation Id** A unique numeric identifier for the separation of duty violation record.

Separation of Duty Configuration namespace

The Separation of Duty Configuration namespace pertains to the configuration attributes of a separation of duty policy. It encompasses the business units, owner, and roles for the separation of duty policy. You can generate the separation of duty policy configuration reports.

Query subjects for Separation of Duty Configuration namespace

The following table lists the query subjects in the Separation of Duty Configuration namespace.

Table 261. Query subjects in the Separation of Duty Configuration namespace

Query subject	Description
Separation of Duty Policy	Represents the separation of duty policy and its configuration attributes. You must us this query subject with the Separation of Duty Rule query subject.

Table 261. Query subjects in the Separation of Duty Configuration namespace (continued)

Query subject	Description
Separation of Duty Rule	Represents the separation of duty rule that is associated with the separation of duty policy.
Separation of Duty Policy Role	Represents the role that is a part of the separation of duty rule. You must us this query subject with the Separation of Duty Rule query subject.

Query items for Separation of Duty Configuration namespace

The following table lists the query items in the Separation of Duty Configuration namespace.

Table 262. Query items in the Separation of Duty Configuration namespace

Query subject	Query items and their description
Separation of Duty Policy	**Separation of Duty Policy Name** The name of the separation of duty policy. **Separation of Duty Policy Description** The description of the separation of duty policy. **Separation of Duty Policy Enabled** Indicates whether the policy is enabled or not. **True** represents Enabled, and **False** represents Disabled. **Separation of Duty Policy Business Unit Name** The name of a business unit to which the separation of duty policy applies. **Separation of Duty Policy Owner Name** the name of the policy owner. The owner can be: • The single or multiple roles. • The single or multiple users. **Separation of Duty Policy Owner Type** The type of an owner for the separation of duty policy. The valid values are Role and Person. **Separation of Duty Policy Owner Business Unit Name** The name of a business unit to which the policy owner belongs. **Separation of Duty Policy Id** A unique numeric identifier for the separation of duty policy. **Separation of Duty Policy Owner Dn** An LDAP distinguished name for an owner of the policy.
Separation of Duty Rule	**Separation of Duty Policy Rule Name** The name of a rule that is associated with the separation of duty policy. **Separation of Duty Policy Rule Max Roles Allowed** The maximum number of the roles that can be a part of the separation of duty rule. **Separation of Duty Rule Id** A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.

Table 262. Query items in the Separation of Duty Configuration namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Role	**Separation of Duty Policy Role Name** The name of the role that is a part of the separation of duty rule. **Separation of Duty Policy Role Description** Describes the separation of duty policy role. **Separation of Duty Policy Business Unit Name** The name of a business unit to which the separation of duty policy role applies. **Separation of Duty Policy Role Dn** An LDAP distinguished name for the role that is a part of the separation of duty policy. **Separation of Duty Policy Role Id** a unique numeric identifier for the role that is a part of separation of duty policy. **Separation of Duty Policy Rule Id** A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.

User Audit namespace

The User Audit namespace contains the query subjects and query items for auditing the user entity.

Query subjects for User Audit namespace

The following table lists the query subjects in the User Audit namespace.

Table 263. Query subjects in the User Audit namespace

Query subject	Description
Person	Represents a person entity and its configuration attributes.
User Audit	Represents the audited actions that apply to the users. You must use this query subject with either the Person or Business Partner Person query subjects or both.
Person Business Unit	Represents the business unit to which a person belongs. You must use this query subject with the Person query subject to obtain the configuration information about the business unit that is associated with the person.
Person Roles	Provides information about the roles for a user of a type person.
Business Partner Person	Represents a business partner person entity and its configuration attributes.
Business Partner Person Business Unit	Represents the business unit to which a business partner person belongs. You must use this query subject with the Business Partner Person query subject to obtain the configuration information about the business unit that is associated with the business partner person.
Business Partner Roles	Represents the roles for a user of a type business partner person.

Query items for `User Audit` namespace

The following table lists the query items in the `User Audit` namespace.

Table 264. List of query items in the `User Audit` namespace

Query subject	Query items and their description
Person	**Person Full Name** The full name of a user. **Person Last Name** The surname of a user. **Person Supervisor** An LDAP distinguished name for the supervisor of a user. **Person Status** The status of a user entity. The valid values are `Active` and `Inactive`. **Person Dn** An LDAP distinguished name for a user. **Person Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs.

Table 264. List of query items in the `User Audit` namespace (continued)

Query subject	Query items and their description
User Audit	**Audit Person Name** The name of a person on which the audit action is performed. **Audit Person Business Unit** The business unit of a person or the business partner person. **Audit Entity Type** The type of a user entity. The valid values are `Person`, `Business Partner Person`, and `System User`. **Audit Action** An action that is performed on a person or the business partner person. For example, `Add`, `Delete`, `Modify`, `Transfer`, `Restore`, `Add Delegate`, and `Suspend`. **Audit Initiator Name** The name of a user who initiates an action on a person or the business partner person. **Audit Process Requestee Name** The entity upon which an audit action is performed. **Audit Process Recertifier** The name of the user who approves the audit process workflow. **Audit Operation Start Time** The date and time when the audit operation on a person or the business partner person started. **Audit Process Submission Time** The audit process submission date and time. **Audit Process Schedule Time** The date and time at which an event is scheduled for the execution. **Audit Process Completion Time** The audit process completion date and time. **Audit Process Result Summary** The result of a person or the business partner person audit process. **Audit Activity Name** The name of an activity that corresponds to the audit process. **Audit Activity Submission Time** The audit activity start date and time. **Audit Activity Completion Time** The audit activity completion date and time. **Audit Activity Result Summary** The result of an activity for a person or the business partner person audit process. **Audit Comments** The comments that are entered by the audit workflow approver. Along with the audit comments, this query item might contain the operational data. **Audit Person Dn** An LDAP distinguished name for a user. **Audit Person Container Dn** An LDAP distinguished name for the parent business unit to which a user belongs.

Table 264. List of query items in the `User Audit` namespace (continued)

Query subject	Query items and their description
Person Business Unit	**Business Unit Name** The name of a business unit. **Business Unit Supervisor** A user who is the supervisor of a business unit. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs. **Business Unit Container Dn** An LDAP distinguished name for the parent business unit of an organization entity.
Person Roles	**Role Name** The name of a role. **Role Type** The type of a role. The valid values are `Static` and `Dynamic`. **Role Dn** An LDAP distinguished name for the role. **Role Container Dn** An LDAP distinguished name for the parent business unit of the role.
Business Partner Person	**Business Partner Person Full Name** The full name of a user. **Business Partner Person Last Name** The surname of a user. **Business Partner Person Supervisor** An LDAP distinguished name for the supervisor of a user. **Business Partner Person Status** The status of a user entity. The valid values are `Active` and `Inactive`. **Business Partner Person Dn** An LDAP distinguished name for a user. **Business Partner Person Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs.
Business Partner Person Business Unit	**Business Unit Name** The name of a business unit. **Business Unit Supervisor** A user who is the supervisor of a business unit. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs. **Business Unit Container Dn** An LDAP distinguished name for the parent business unit of an organization entity.

Table 264. List of query items in the User Audit namespace (continued)

Query subject	Query items and their description
Business Partner Roles	**Role Name** The name of a role. **Role Type** The type of a role. The valid values are Static and Dynamic. **Role Dn** An LDAP distinguished name for the role. **Role Container Dn** An LDAP distinguished name for the parent business unit of the role.

User Configuration namespace

The User Configuration namespace contains the query subjects and query items for configuring the user entity.

Query subjects for User Configuration namespace

The following table lists the query subjects in the User Configuration namespace.

Table 265. Query subjects in the User Configuration namespace

Query subject	Description
Person	Represents a person entity and its configuration attributes.
Person Aliases	Provides information about the user aliases.
Person Manager	Provides information about the manager of a user.
Account	Represents an account entity and its configuration attributes. You must use this query subject with the Person query subject to obtain information about the accounts that are owned by the user.
Role	Represents the role entity and its configuration attributes. You must use this query subject with the Person query subject to obtain information about the role membership for a user.
Person ACI	Represents an ACI that is applicable to a user. You must use this query subject with the Person query subject to obtain information about an ACI applicable to the user.
ACI Operations	Represents the operations that an ACI governs. You must use this query subject with the Person ACI query subject to obtain information about an ACI associated with the user.
ACI Attribute Permissions	Represents the attributes and operations that can be performed on an attribute. You must use this query subject with the Person ACI query subject to obtain information about an ACI associated with the user.
ACI Members	Provides information about the members of an ACI. You must use this query subject with the Person ACI query subject to obtain information about the ACI members.
Supervised Business Unit	Represents the business unit entity that a user supervises and its configuration attribute. You must use this query subject with the Person query subject to obtain information about the business unit a user supervises.
Service Ownership	Represents the service entity that a user owns. You must use this query subject with the Person query subject to obtain information about the services that the user own.
Roles Ownership	Represents the role entity that a user owns. You must use this query subject with the Person query subject to obtain information about the roles that the user own.

Table 265. Query subjects in the `User Configuration` namespace (continued)

Query subject	Description
Group Ownership	Represents the group entities that a user own. You must use this query subject with the `Person` query subject to obtain information about the groups that the user owns.
Credential Pool Ownership	Represents the credential pool that a user owns. You must use this query subject with the `Person` query subject to obtain information about the credential pool that the user owns.
Separation of Duty Policy Ownership	Represents the separation of duty policies that a user own. You must use this query subject with the `Person` query subject to obtain information about the separation of duty policies that the user own.

Query items for `User Configuration` namespace

The following table lists the query items in the `User Configuration` namespace.

Table 266. List of query items in the `User Configuration` namespace

Query subject	Query items and their description
Person	**Person Full Name** The full name of a user. **Person Last Name** The surname of a user. **Person Preferred User ID** Represents the name that a user might prefer during an account creation. **Person Email** An email address of a user. **Person Status** The status of the user entity. The valid values are `Active` and `Inactive`. **Person Business Unit Name** The name of the business unit to which a user belongs. **Person Administrative Assistant Dn** An LDAP distinguished name for the administrative assistant of a user. **Person Dn** An LDAP distinguished name for a user. **Person Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs. **Person Business Unit Supervisor** An LDAP distinguished name for the supervisor of the business unit to which a user belongs.
Person Aliases	**Person Alias Name** The name of a user alias. **Person Dn** An LDAP distinguished name for the user to which an alias belongs.

Table 266. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
Person Manager	**Person Full Name** The full name of the manager. **Person Last Name** The surname of the manager. **Person Status** The status of the manager entity. The valid values are `Active` and `Inactive`. **Person Dn** An LDAP distinguished name for the manager. **Person Business Unit Dn** An LDAP distinguished name for the business unit to which a manager belongs. **Person Supervisor** The user supervisor of the manager.

Table 266. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
Account	**Account Name** The name of an account. **Account Status** The status of an account. The valid values are `Active` and `Inactive`. **Account Compliance** The compliance status of an account. The valid values are `Unknown`, `Compliant`, `Disallowed`, and `Non Compliant`. **Account Ownership Type** The ownership type of an account. The valid values are `Individual`, `System`, `Device`, and `Vendor`. **Account Last Access Date** The last accessed date of an account. **Account Service Name** The name of the service on which an account is provisioned. **Account Service Type** The profile of the service on which an account is provisioned. **Account Service Url** A URL that connects to the service on which an account is provisioned. **Account Service Business Unit Name** An LDAP distinguished name for the business unit to which a service belongs. **Account Dn** An LDAP distinguished name for an account. **Account Service Dn** An LDAP distinguished name for the service on which an account is provisioned. **Account Service Business Unit Dn** An LDAP distinguished name for the business unit to which a service belongs. **Account Service Owner Dn** An LDAP distinguished name for a user who is the owner of the service. **Account Service Business Unit Supervisor Dn** An LDAP distinguished name for the supervisor of the business unit to which a service belongs. **Account Owner Business Unit Dn** An LDAP distinguished name for the business unit of a user who owns the account.

Table 266. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
Role	**Role Name** The name of a role. **Role Description** The description of a role. **Role Type** The type of a role. The valid values are `Static` and `Dynamic`. **Role Access Enabled** Represents whether or not access for a role is enabled. **`True`** represents Enabled, and **`False`** represents Disabled. **Role Common Access Enabled** Represents whether or not common access for the role is enabled. The valid values are `True` and `False`. **Role Access Type** The type of an access that is enabled for a role. **Role Dn** An LDAP distinguished name for the role. **Role Business Unit Dn** An LDAP distinguished name for the business unit of a role.
Person ACI	**ACI Name** The name of the Access Control Item (ACI). **ACI Protection Category** The category of an entity that an ACI protects. The value of this item must be `Person`. **ACI Target** The type of the selected protection category that is associated with an ACI. The valid values are `inetOrgPerson` and `erPersonItem`. **ACI scope** The scope of an ACI. It determines whether an ACI is applicable to subunits of a business organization or not. The valid values and their meanings: • `single` - The policy applies to a business unit and not its subunits. • `subtree` - The policy applies to the subunits of a business organization. **ACI Business Unit Dn** An LDAP distinguished name for the business unit on which an ACI is defined.
ACI Operations	**ACI Operation Name** The name of an operation that an ACI governs. **ACI Operation Permission** The permission that applies to an ACI operation. The valid values are `grant`, `deny`, and `none`. **ACI Business Unit Dn** An LDAP distinguished name for the business unit.

Table 266. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
ACI Attribute Permissions	**ACI Attribute Name** The name of an attribute for which an ACI controls the permissions. **ACI Attribute Operation** The name of an operation that can be run on an attribute. The valid values are **r** for read operation, **w** for write operation, and **rw** for read and write operations. **ACI Attribute Permission** The permission that applies to an ACI operation. The valid values are `grant` and `deny`. **ACI Business Unit Dn** An LDAP distinguished name for the business unit.
ACI Members	**ACI Member Name** The members that an ACI governs. The valid values are: • `All Users` - All users in the system. • `Profile Owner` - The owner of the profile. • `Manager` - The manager of the profile owner. • `Sponsor` - The sponsor of the Business Partner organization in which the person resides. • `Administrator` - The administrator of the domain in which the person resides. • `Service Owner`- The owner of the service. • `Access Owner` - The owner of an access. **ACI System Group Name** Represents the name of the group whose members are governed by an ACI. **ACI Business Unit Dn** An LDAP distinguished name for the business unit. **ACI System Group Dn** An LDAP distinguished name for the system group.
Supervised Business Unit	**Business Unit Name** The name of a business unit. **Business Unit Supervisor** A user who is the supervisor of a business unit. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs. **Business Unit Container Dn** An LDAP distinguished name for the parent business unit of an organization entity.

Table 266. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
Service Ownership	**Service Name** The name of a service to which the accounts are provisioned. **Service Dn** An LDAP distinguished name for the service. **Service Container Dn** An LDAP distinguished name for the business unit of a service. **Service Owner Dn** An LDAP distinguished name for a user who owns the service. **Service Url** A URL that connects to the managed resource. **Service Type** The service profile type.
Roles Ownership	**Role Name** The name of a role. **Role Description** The description of a role. **Role Type** The type of a role. The valid values are `Static` and `Dynamic`. **Role Access Enabled** Represents whether an access for a role is enabled or not. **`True`** represents Enabled, and **`False`** represents Disabled. **Role Common Access Enabled** Represents whether or not common access for the role is enabled. The valid values are `True` and `False`. **Role Access Type** The type of an access that is enabled for a role. **Role Dn** An LDAP distinguished name for a role. **Role Business Unit Dn** An LDAP distinguished name for the business unit of a role.

Table 266. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
Group Ownership	**Group Name** The name of a group for which an access is defined. **Group Type** The profile type of a group. **Group Access Name** The name of an access that is defined for a group. **Group Access Type** The type of an access that is defined for a group. **Group Service Name** The name of a service on which the group is provisioned. **Group Service Type** The profile type of a service on which the group is provisioned. **Group Service Url** A URL that connects to the service to which the group is provisioned. **Group Service Business Unit Name** The name of a business unit to which the service belongs. **Group Dn** An LDAP distinguished name for a group entity to which an access is defined. **Group Service Dn** An LDAP distinguished name for the service that is associated to a group. **Group Service Business Unit Dn** An LDAP distinguished name for the business unit to which a service belongs. **Group Service Owner Dn** An LDAP distinguished name for a user who owns the service. **Group Service Business Unit Supervisor** An LDAP distinguished name for the supervisor of a business unit to which a service belongs.
Credential Pool Ownership	**Credential Pool Name** The name of a credential pool. **Credential Pool Service Dn** An LDAP distinguished name for a service to which the group associated with a credential pool is provisioned. **Credential Pool Business Unit Dn** An LDAP distinguished name for the business unit of a credential pool. **Credential Pool Dn** An LDAP distinguished name for the credential pool.

Table 266. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Ownership	**Separation of Duty Policy Name** The name of the separation of duty policy. **Separation of Duty Policy Description** The description of the separation of duty policy. **Separation of Duty Policy Enabled** Indicates whether or not the policy is enabled. **`True`** represents Enabled, and **`False`** represents Disabled. **Separation of Duty Policy Business Unit Name** The name of a business unit to which the separation of duty policy applies. **Separation of Duty Policy Id** A unique numeric identifier for the separation of duty policy.

`Service Audit` namespace

The `Service Audit` namespace pertains to the audit history of the actions that are performed on the services. You can generate the audit reports for the various types of services.

Query subjects for `Service Audit` namespace

The following table lists the query subjects in the `Service Audit` namespace.

Table 267. Query subjects in the `Service Audit` namespace

Query subject	Description
Service	Represents the service and its configuration attributes on which the audit actions are performed. **Note:** You cannot see the deleted services by using this query subject.
Service Audit	Represents the audited actions applicable to the services. You must use this query subject with the `Service` query subject. **Note:** You can use this query subject alone to report any deletion of the previously existing services.
Service Health	Represents the status of a resource on which the service is created. You must use this query subject with the `Service` query subject.
Service Provisioning Policy	Represents the provisioning policies that are applied on the service. You must use this query subject with the `Service` query subject.

Query items for `Service Audit` namespace

The following table lists the query items in the `Service Audit` namespace.

Table 268. List of query items in the `Service Audit` namespace

Query subject	Query items and their description
Service	**Service Name** The name of a service. **Service Type** The type of a service. For example, `PosixLinuxProfile`. **Service Description** The description of the service that is entered during the service creation or modification. **Service Business Unit Name** The business unit to which a service belongs. **Service Url** The IP address of the resource on which the service is created. **Service Tag** A tag that logically groups the services. If a service is tagged during creation or modification, this query item represents the name of the tag. **Service Owner First Name** The given name of a user who is the service owner. **Service Owner Last Name** The surname of a user who is the service owner. **Service Owner Business Unit Dn** An LDAP distinguished name for a business unit to which the service owner belongs. **Service Dn** An LDAP distinguished name for a service.

Table 268. List of query items in the `Service Audit` namespace (continued)

Query subject	Query items and their description
Service Audit	**Audit Service Name** The name of a service on which the audit action is run. **Audit Service Business Unit** The business unit of a service. **Audit Action** Represents an action that is run on the service. The possible values are: • `Add`. • `Delete`. • `Modify`. • `EnforcePolicyForService`. • `UseGlobalSetting`. • `CorrectNonCompliant`. • `SuspendNonCompliant`. • `AlertNonCompliant`. • `MarkNonCompliant`. **Audit Comments** The comments that are entered by the audit workflow approver. Along with the audit comments, this query item might contain the operational data. **Audit Initiator Name** The name of a user who initiates the action on the service. **Audit Process Requestee Name** The entity upon which an audit action is run. **Audit Operation Start Time** The start date and time when the operation on the service started. **Audit Process Submission Time** The date and time of the audit process submission. **Audit Process Schedule Time** The date and time at which an event is scheduled for the execution. **Audit Process Completion Time** The date and time of the audit process completion. **Audit Process Subject** The subject on which the audit action is run. It applies to the cases where the defined workflow must complete before the audit action is complete. **Audit Process Subject Profile** The profile type of an entity that is associated with the audit action. This query item contains a value only if the `Audit Process Subject` contains the value. **Audit Process Result Summary** The result of the audit process on the service that is indicated with the values such as `Success` or `Failed`.

Table 268. List of query items in the `Service Audit` namespace (continued)

Query subject	Query items and their description
Service Health	**Resource Dn** An LDAP distinguished name for the service. **Resource Status** Indicates whether or not resource that is represented by the service is available. The valid values are `Success` and `Failed`. **Resource Test Status** Indicates whether or not resource that is represented by the service is connectable. The valid values are `Success` and `Failed`. **Last Response Time** The date and time of the last received response from the resource that is represented by the service. **Lock Service** Shows if a service is locked. For example, `Service is locked for the reconciliation.` **Last Reconciliation Time** The last date and time when the reconciliation of the service is attempted either by the system or through an explicit request of the reconciliation. **Server** The application server on which the service that pertains to a resource is created. The details are up to the level of a node on which the service is created. **Restart Time** The time from the last restart of a server. **First Resource Fail Time** The date and time when the resource fails for the first time. Use this information to analyze the resource failure situations.
Service Provisioning Policy	**Provisioning Policy Name** The name of a provisioning policy that applies to a service. **Provisioning Policy Scope** The scope in terms of a hierarchy of the business units to which the provisioning policy applies. The valid values and their meanings: • `Single` - The policy applies to a business unit and not its subunits. • `Subtree` - The policy applies to the business unit and its subunits. **Provisioning Policy Is Enabled** Represents whether the provisioning policy is enabled or not. **`True`** represents Enabled, and **`False`** represents Disabled. **Provisioning Policy Dn** An LDAP distinguished name for the provisioning policy. **Provisioning Policy Business Unit Dn** An LDAP distinguished name for the business unit to which the provisioning policy applies.

Access Audit namespace

The Access Audit namespace pertains to the audit history of the actions that are performed on the access entities. The access audit is currently supported only for the group that is defined as an access.

Query subjects for Access Audit namespace

The following table lists the query subjects in the Access Audit namespace.

Table 269. Query subjects in the Access Audit namespace

Query subject	Description
Access Audit	Represents the audit history of the access entity. You must use this query subject with the Access query subject.
Access	Represents the access entity on which the audit actions are performed. This query subject also contains the configuration attributes of an access.
Access Owner	Represents a user who owns the access.
Access Owner Business Unit	Represents the business unit to which an access owner belongs. You must use this query subject with the Access Owner query subject to obtain the configuration information about the business unit that is associated with an owner.
Access Service	Represents the service on which the access is provisioned. You must use this query subject with the Access query subject to obtain the configuration information about the access service.
Access Service Business Unit	Represents the business unit to which a service belongs. You must use this query subject with the Access Service query subject to obtain the configuration information about the business unit that is associated with the service.
Access Members	Provides information about the accounts that are the members of an access.
Access Member Owner	Provides information about the users who own the accounts that are members of an access.
Access Member Owner Business Unit	Represents the business unit to which the access member owner belongs.

Query items for Access Audit namespace

The following table lists the query items in the Access Audit namespace.

Table 270. List of query items in the Access Audit namespace

Query subject	Query items and their description
Access Audit	**Audit Access Name** The name of an access on which the audit operation is run. **Audit Access Service Name** The name of a service for which the access is defined. **Audit Action** An action that is run on the access. The valid values are: • Add. • Modify. • Delete. • AddMember. • RemoveMember. **Audit Initiator Name** The name of a user who initiates the audit action. For the audit actions such as AddMember and RemoveMember, the initiator name represents the name of IBM Security Identity Manager account. **Audit Account Name** The name of an account for which the access is either requested or deleted. This query item applies to only AddMember and RemoveMember audit actions. **Audit Process Requestee Name** The name of a user whose account is added to the access. This query item applies to only AddMember and RemoveMember audit actions. **Audit Process Recertifier Name** The name of a user who approves the audit action. **Audit Operation Start Time** The audit operation start date and time. **Audit Activity Owner** IBM Security Identity Manager account user name that owns the activity. For example, a user who approves the request to add an account to the access. **Audit Activity Name** The name of the audit activity. **Audit Activity Start Time** The audit activity start date and time. **Audit Activity Completion Time** The audit activity completion date and time. **Audit Process Submission Time** The audit process submission date and time. **Audit Process Schedule Time** The date and time at which an event is scheduled for the execution. **Audit Process Completion Time** The audit process completion date and time. **Audit Activity Result Summary** The result of an activity within a role audit process. **Audit Comments** The comments that are entered by the audit workflow approver. **Audit Process Result Summary** The result of the access audit process.

Table 270. List of query items in the `Access Audit` namespace (continued)

Query subject	Query items and their description
Access	**Group Name** The name of a group for which the access is defined. **Group Type** The profile type of a group. **Group Access Name** The name of an access that is defined for a group. **Group Access Type** The type of an access that is defined for a group. **Group Supervisor** The name of a user who is the supervisor of a group. **Group Dn** An LDAP distinguished name for a group to which the access is defined. **Group Container Dn** An LDAP distinguished name for the business unit that is associated with a group. **Group Owner Dn** An LDAP distinguished name for a group owner. **Group Service Dn** An LDAP distinguished name for the service that is associated with a group. **Group Access Defined** Specifies whether or not access is defined for a group. The possible values are `True` and `False`. **Group Access Enabled** Specifies whether or not access is enabled for a group. The possible values are `True` and `False`. **Group Common Access Enabled** Specifies whether or not common access is enabled for a group. The possible values are `True` and `False`.
Access Owner	**Access Owner Full Name** The given name of an account owner. **Access Owner Last Name** The surname of an account owner. **Access Owner Status** The status of a user. The valid values are `Active` and `Inactive`. **Access Owner Dn** An LDAP distinguished name for an account owner. **Access Owner Business Unit Dn** An LDAP distinguished name for the business unit to which an account owner belongs. **Access Owner Manager Dn** An LDAP distinguished name for the user supervisor of the account owner.

Table 270. List of query items in the `Access Audit` namespace (continued)

Query subject	Query items and their description
Access Owner Business Unit	**Business Unit Name** The name of a business unit. **Business Unit Supervisor** The business unit of a user who is the supervisor. **Business Unit Dn** An LDAP distinguished name for the business unit. **Business Unit Container Dn** An LDAP distinguished name for the parent business unit.
Access Service	**Service Name** The name of a service to which the access belongs. **Service Dn** An LDAP distinguished name for a service to which the access belongs. **Service Container Dn** An LDAP distinguished name for a business unit of a service that is associated with the access. **Service Owner Dn** An LDAP distinguished name for a user owner of the service. **Service URL** A URL that connects to the managed resource. **Service Type** The service profile type.
Access Service Business Unit	**Business Unit Name** The name of a business unit. **Business Unit Supervisor** A user who is the supervisor of a business unit. **Business Unit Dn** An LDAP distinguished name for a business unit. **Business Unit Container Dn** An LDAP distinguished name for the parent business unit.

Table 270. List of query items in the `Access Audit` namespace (continued)

Query subject	Query items and their description
Access Members	**Account Name** The name of an account that is a member of an access. **Account Ownership Type** The type of the account ownership. The valid values are: • `Device`. • `Individual`. • `System`. • `Vendor`. **Account Status** The status of an account. The valid values are `Active` and `Inactive`. **Account Compliance** Indicates whether an account is compliant or not. The valid values are: • `Unknown`. • `Compliant`. • `Non Compliant`. • `Disallowed`. **Account Last Access Date** The last accessed date and time of an account. **Account Dn** An LDAP distinguished name for an account. **Account Service Dn** An LDAP distinguished name for a service to which the account belongs.
Access Member Owner	**Person Full Name** The full name of an account owner. **Person Last Name** The surname of an account owner. **Person Dn** An LDAP distinguished name for an account owner. **Person Business Unit Dn** An LDAP distinguished name for the business unit to which an account owner belongs. **Person Supervisor** A user who is the supervisor of an account owner.
Access Member Owner Business Unit	**Business Unit Name** The name of a business unit to which the account owner belongs. **Business Unit Supervisor** A user who is the supervisor of a business unit. **Business Unit Dn** An LDAP distinguished name for a business unit. **Business Unit Container Dn** An LDAP distinguished name for the parent business unit of an organization entity.

Access Configuration namespace

Use the Access Configuration namespace to view access configuration and its business metadata for the access entities.

Query subjects for Access Configuration namespace

The following table lists the query subjects in the Access Configuration namespace.

Table 271. Query subjects in the Access Configuration namespace

Query subject	Description
Access	Represents an access that is defined in an organization. You can use this query subject with either of the following query subjects to obtain the business metadata for each access: • Service Business Meta Data. • Group Business Meta Data. • Role Business Meta Data.
Service	Represents the services that are defined in an organization with its configuration attributes. You can use this query subject with either of the following query subjects to view the service that is defined as an access: • Access. • Service Business Meta Data.
Service Business Meta Data	Represents the business metadata of the service that is defined as an access.
Group	Represents the groups that are defined in an organization with its configuration attributes. You can use this query subject with either of the following query subjects to view the groups that are defined as an access: • Access. • Group Business Meta Data.
Group Access Owner	Represents a user who owns the group access. The query subject shows a unified view of a Person and Business Partner Person.
Group Business Meta Data	Represents the business metadata of the group that is defined as an access.
Role	Represents the role that is defined in an organization with its configuration attributes.
Role Business Meta Data	Represents the business metadata of the role that is defined as an access.
Business Partner Person	Represents the business partner person entity and its configuration attributes.
Person	Represents a person entity and its configuration attributes.
User	Represents the entitlements of an individual in the organization. These entitlements can be role, groups, or services that are defined as access to which the user is entitled.

Query items for Access Configuration namespace

The following table lists the query items in the Access Configuration namespace.

Table 272. List of query items in the Access Configuration namespace

Query subject	Query items and their description
Access	**Entity Name** The name of a role, service, or group that is defined as an access. **Access Name** The name of the access that is defined in an organization. **Access Category** The category of the access application, email group, role, shared folder, or any other custom category that is defined. **Access Type** The type of an access. The type of an access can be a role, group, or service. **Access Dn** An LDAP distinguished name for an access.
Service Business Meta Data	**Access ID** A unique identifier that represents the business metadata for a service that is defined as an access. **Access Description** The description of a service that is defined as an access. **Access Icon Url** A uniform resource identifier (URL) string for the icon that represents an access. **Access Additional Information** Displays information about the access card by default. It is an extra information about the access item that an administrator can use. **Access Badge Style** Represents the class that applies the formatting to the badge text such as, font type, size, or color. **Access Badge Text** Provides the details about the badge that is defined for an access.
Group	**Group Name** The name of the group that is defined in an organization. **Group Type** The profile type of a group. **Group Dn** An LDAP distinguished name for a group. **Group Business Unit Dn** An LDAP distinguished name for the business unit of a group. **Group Owner Dn** An LDAP distinguished name of an owner that owns the group. **Group Service Dn** An LDAP distinguished name of a service to which the group belongs.

Table 272. List of query items in the `Access Configuration` namespace (continued)

Query subject	Query items and their description
Group Business Meta Data	**Access Name** The name of an access of a type as group. **Access Description** The description of a group that is defined as an access. **Access Icon Url** A uniform resource identifier (URL) string for the icon that represents an access. **Access Additional Information** Displays information about the access card by default. It is an extra information about the access item that an administrator can use. **Access Badge Style** Represents the class that applies the formatting to the badge text such as, font type, size, or color. **Access Badge Text** Provides the details about the badge that is defined for an access. **Access ID** A unique identifier that represents the business metadata for a group that is defined as an access.
Service	**Service Name** The name of the service or resource that is defined in an organization. **Service Type** The type of a service. For example, `PosixLinuxProfile`. **Service Dn** An LDAP distinguished name for a service. **Service Business Unit Dn** An LDAP distinguished name for a business unit of a service. **Service ID** A unique identifier that represents the service.
Role	**Role Name** The name of a role. **Role Type** The type of a role. The valid values are `Static` and `Dynamic`. **Role Dn** An LDAP distinguished name for a role. **Role Business Unit Dn** An LDAP distinguished name for the business unit of a role. **Role Supervisor** The supervisor of a user for the business unit of a role. **Role Owner Dn** An LDAP distinguished name for the role owner. **Role Parent Dn** An LDAP distinguished name for the parent role.

Table 272. List of query items in the `Access Configuration` namespace (continued)

Query subject	Query items and their description
Role Business Meta Data	**Access Name** The name of an access of a type as role. **Access Description** The description of a role that is defined as an access. **Access Icon Url** A uniform resource identifier (URL) string for the icon that represents an access. **Access Additional Information** Displays information about the access card by default. It is an extra information about the access item that an administrator can use. **Access Badge Style** Represents the class that applies the formatting to the badge text such as, font type, size, or color. **Access Badge Text** Provides the details about the badge that is defined for an access. **Access ID** A unique identifier that represents the business metadata for a role that is defined as an access.
Business Partner Person	**Business Partner Person Full Name** The full name of a user. **Business Partner Person Last Name** The surname of a user. **Business Partner Person Supervisor** An LDAP distinguished name for the supervisor of a user. **Business Partner Person Status** The status of a user entity. The valid values are `Active` and `Inactive`. **Business Partner Person Dn** An LDAP distinguished name for a user. **Business Partner Person Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs. **Business Partner Person Parent** The name of the parent business partner person.
Person	**Person Full Name** The full name of a person. **Person Last Name** The surname of a person. **Person Status** The status of a person entity. The valid values are `Active` and `Inactive`. **Person Business Unit Supervisor** An LDAP distinguished name for the supervisor of the business unit to which a person belongs. **Person Dn** An LDAP distinguished name for a person. **Person Business Unit Dn** An LDAP distinguished name for the business unit to which a person belongs.

Table 272. List of query items in the `Access Configuration` namespace (continued)

Query subject	Query items and their description
Group Access Owner	**Full Name** The full name of a user. **Last Name** The surname of a user. **Type** The type of a user. For example, `Person` or `Business Partner Person`. **Dn** An LDAP distinguished name for a user. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs.
User	**User Dn** An LDAP distinguished name for a user with defined access on Role, Group, or Service. **User Name** The full name of the user with defined access on Role, Group, or Service. **User Last Name** The surname of the user with defined access on Role, Group, or Service. **User Type** The profile type of the user with defined access on Role, Group, or Service. **User Business Unit Dn** An LDAP distinguished name for the business unit to which a user, with defined access on Role, Group, or Service, belongs. **User Business Unit Name** The name of the business unit to which a user, with defined access on Role, Group, or Service, belongs.

Index

A

access
  configuration, namespace 242
  configuration, query items 243
  configuration, query subjects 242
access audit
  namespace 237
  query items 238
  query subjects 237
Access catalog tables 56
access request management 125
  AUDIT_EVENT values 129
  AUDIT_MGMT_ACCESS_REQUEST values 126
  AUDIT_MGMT_MESSAGE values 129
  AUDIT_MGMT_OBLIGATION values 127
  AUDIT_MGMT_OBLIGATION_ATTRIB values 118, 128, 142
  AUDIT_MGMT_OBLIGATION_RESOURCE values 119, 129, 142
account
  audit, namespace 183
  audit, query items 184
  audit, query subjects 183
  configuration, namespace 187
  configuration, query items 189
account management 139
ACCT_CHANGE table 35
ACI
  management 124
  management events 124
  table 26
ACI_CATEGORIES table 77
ACI_PERMISSION_ATTRIBUTERIGHT table 27
ACI_PERMISSION_CLASSRIGHT table 27
ACI_PRINCIPALS table 27
ACI_ROLEDNS table 26
ACTIVITY table 8
ACTIVITY_LOCK table 15
ATTR_CHANGE table 36
attributes 165
  mapping 165
AUDIT_EVENT 114
  access request management 129
  create manual activity event 135
  escalate manual activity event 138
  lifecycle rule 138
AUDIT_EVENT table 125, 140, 143, 150, 158
  column values 115, 116, 120, 124, 140, 143, 144, 146, 148, 150, 151, 152, 153, 154, 156, 157
  table columns 115, 117, 120, 121, 125, 130, 138, 139, 140, 143, 145, 147, 148, 150, 151, 152, 153, 154, 155, 157, 158
AUDIT_MGMT_ACCESS_REQUEST
  access request management 126
AUDIT_MGMT_ACTIVITY
  create manual activity event 131
  escalate manual activity event 136
AUDIT_MGMT_DELEGATE 119
AUDIT_MGMT_MESSAGE
  access request management 129
AUDIT_MGMT_OBLIGATION
  access request management 127
AUDIT_MGMT_OBLIGATION_ATTRIB
  access request management 118, 128, 142
AUDIT_MGMT_OBLIGATION_RESOURCE
  access request management 119, 129, 142
AUDIT_MGMT_PARTICIPANT
  create manual activity 134
  escalate manual activity 136
AUDIT_MGMT_PROVISIONING table 139
AUDIT_MGMT_TARGET 116
AUDIT_MGMT_TARGET table 124, 144, 146, 149
AUDIT_MGNT_TARGET table 148
auditing schema tables 113
AUTH_KEY table 77
authentication 115
AUTHORIZATION_OWNERS table 26

B

BULK_DATA_INDEX table 21
BULK_DATA_SERVICE table 21
BULK_DATA_STORE table 21

C

CHANGELOG table 30
COLUMN_REPORT table 25
COMMON_TASKS table 77
COMPLIANCE_ALERT table 37
container management 143
create manual activity 130
  AUDIT_MGMT_PARTICIPANT values 134
create manual activity event
  AUDIT_EVENT values 135
  AUDIT_MGMT_ACTIVITY values 131
Credential Lease management
  AUDIT_MGMT_LEASE 161
  column values 161
  table columns 162
Credential management 159
  column values 159
  table columns 159
Credential Pool management 160, 161
  column values 160
  table columns 160

D

database tables 1
database view tables 70
DB_REPLICATION_CONFIG table 43
delegate authority 119
directory tree 81

E

entities 165
  mapping 165
ENTITLEMENT table 28
Entitlement workflow management 16, 148, 152
ENTITLEMENT_PROVISIONING PARAMS table 28
entity operation management 153
ENTITY_COLUMN table 24
entity_name column values 155
erAccessItem 94
erAccessType 94
erAccountItem 94
erAccountTemplate 107
erADJNDIFeed 96
erAdoptionPolicy 107
erAttributeConstraint 97
erBPOrg 84
erBPOrgItem 85
erBPPersonItem 83
erChallenges 97
erComplianceIssue 98
ERCREDENTIALLEASE table 42
erCSVFeed 98
erDictionary 85
erDictionaryItem 85
erDSML2Service 99
erDSMLInfoService 99
erDSMLInfoService attributes
  erDSMLFileName 99
  erEvaluateSoD 99
  erPassword 99
  erPlacementRule 99
  erproperties 99
  erprotocolmappings 99
  erServiceName 99
  erserviceproviderfactory 99
  erUid 99
  erUseWorkflow 99
  erxforms 99
erDynamicRole 85
erFormTemplate 86
erGroupItem 100
erHostedAccountItem 100
erHostedService 101
erHostSelectionPolicy 101
erIdentityExclusion 86
erIdentityPolicy 107
erITIMService 101
erJNDIFeed 101
erJoinDirective 102

erLifecycleProfile 104
erLocationItem 86
erManagedItem 86
erObjectCategory 103
erObjectProfile 103
erOrganizationItem 87
erOrgUnitItem 87
erOwnershipType class 93
erPasswordPolicy 107
erPersonItem 88
erPolicyBase 108
erPolicyItemBase 108
erPrivilegeRule 102
erProvisioningPolicy 108
erRecertificationPolicy 109
erRemoteServiceItem 104
erRole 89
erSecurityDomainItem 89
erSeparationOfDutyPolicy 110
erSeparationOfDutyRule 110
erServiceItem 104
erServiceProfile 105
erSystemItem 106
erSystemRole 106
erSystemUser 106
erTemplate 90
erTenant 91
erWorkflowDefinition 93
escalate manual activity 130, 135
  AUDIT_MGMT_PARTICIPANT values 136
escalate manual activity event
  AUDIT_EVENT values 138
  AUDIT_MGMT_ACTIVITY values 136

G

General classes 83
group management 149

I

I18NMESSAGES table 22
import and export tables 21
ITIM group management
  account management events 146
  table 146

L

LCR_INPROGRESS_TABLE table 77
lifecycle rule 138
  AUDIT_EVENT values 138
LISTDATA table 15

M

MANUAL_SERVICE_RECON ACCOUNTS table 19
migration 158
MIGRATION_STATUS table 22

N

namespace
  access audit 237
  access configuration 242
  account audit 183
  account configuration 187
  audit 165
  configuration 165
  provisioning policy audit 196
  provisioning policy configuration 199
  recertification audit 167
  recertification configuration 176
  role audit 203
  role configuration 206
  separation of duty audit 213
  separation of duty configuration 219
  service audit 233
  user audit 221
  user configuration 225
NEXTVALUE table 13

O

organization role management 144

P

PASSWORD_SYNCH table 13
PASSWORD_TRANSACTION table 13
PENDING table 14
PENDING_APPROVAL view 70
person management 116
PERSON_ROLE_ASSIGNMENT table 32
PERSON_ROLE_ASSIGNMENT_VALUES table 32
PO_NOTIFICATION_HTMLBODY TABLE 24
PO_NOTIFICATION_TABLE table 23
PO_TOPIC_TABLE table 23
policy
  classes 107
  management 120
  provisioning policy tables 33
  recertification tables 38
  separation of duty tables 72
policy tables
  recertification 38
  separation of duty 72
POLICY_ANALYSIS 33
POLICY_ANALYSIS_ERROR 34
Post office tables 22
PROCESS table 1
PROCESS_VIEW view 72
PROCESSDATA table 7
PROCESSLOG table 4
provisioning policy audit
  namespace 196
  query items 198
  query subjects 196
provisioning policy configuration
  namespace 199
  query items 200
  query subjects 200

Q

query items 165
  access audit 238
  access configuration 243
  account audit 184
  account configuration 189
  provisioning policy audit 198
  provisioning policy configuration 200
  recertification audit 168
  recertification configuration 177
  role audit 204
  role configuration 208
  separation of duty audit 215
  separation of duty configuration 220
  service audit 234
  user audit 222
  user configuration 226
query subjects 165
  access audit 237
  access configuration 242
  account audit 183
  account configuration 187
  provisioning policy audit 196
  provisioning policy configuration 200
  recertification audit 167
  recertification configuration 176
  role audit 203
  role configuration 206
  separation of duty audit 214
  separation of duty configuration 219
  service audit 233
  user audit 221
  user configuration 225

R

recertification audit
  namespace 167
  query items 168
  query subjects 167
recertification configuration
  namespace 176
  query items 177
  query subjects 176
recertification policy tables 38
RECERTIFICATIONLOG table 38
RECERTIFIER_DETAILS_INFO table 31
Reconciliation 152
RECONCILIATION table 30
RECONCILIATION_INFO table 31
REMOTE_RESOURCES_RECON QUERIES table 19
REMOTE_RESOURCES_RECONS table 18
REMOTE_SERVICES_REQUESTS table 17
Report table 25
reports 24
RESOURCE_PROVIDERS table 16
RESOURCES_SYNCHRONIZATIONS table 29
role assignment attribute tables 32
role audit
  namespace 203

role audit *(continued)*
query items 204
query subjects 203
role configuration
namespace 206
query items 208
query subjects 206
ROLE_ASSIGNMENT_ATTRIBUTES table 33
ROLE_INHERITANCE table 78
ROOTPROCESSVIEW 70
runtime events 156

S

SA_BULK_LOAD table 44
SA_CREDPOOL_DESCRIPTION table 44
SA_CREDPOOL_GROUP table 44
SA_CREDPOOL_OWNER table 45
SA_EVAL_CRED_DESCRIPTION table 47
SA_EVALUATION_BU table 45
SA_EVALUATION_BU_HIERARCHY table 45
SA_EVALUATION_CREDENTIAL table 46
SA_EVALUATION_CREDENTIAL_POOL table 47
SA_EVALUATION_SERVICE table 48
SA_EVALUATION_SERVICE_TAG table 49
SA_GLOBAL_CONFIGURATION table 49
SA_POLICY table 50
SA_POLICY_DESCRIPTION table 51
SA_POLICY_ENTITLEMENT table 51
SA_POLICY_ERURI table 52
SA_POLICY_MEMBERSHIP table 52
SA_VAULT_SERVICE table 53
SA_VAULT_SERVICE_ALIAS table 53
SCHEDULED_MESSAGE table 78
schema
access request management 125
create manual activity 130
escalate manual activity 130, 135
lifecycle rule 138
schema mapping 165
SCRIPT table 20
SecurityDomain 90
self-password change 157
separation of duty audit
namespace 213
query items 215
query subjects 214
separation of duty configuration
namespace 219
query items 220
query subjects 219
separation of duty policy tables 72
service audit
namespace 233
query items 234
query subjects 233
service classes 93
service policy enforcement 151
SERVICE_ACCOUNT_MAPPING table 31
Shared Access tables 42
SOD_OWNER table 72
SOD_POLICY table 73
SOD_RULE table 73
SOD_RULE_ROLE table 74
SOD_VIOLATION_HISTORY table 74
SOD_VIOLATION_ROLE_MAP table 76
SOD_VIOLATION_STATUS table 75
SUBPROCESSVIEW 70
SUSPENDED_ACCOUNT_OPERATIONS view 72
SUSPENDED_USERS view 71
SYNCH_OBJECT_LOCK table 54
SYNCH_POINT table 14
SYNCHRONIZATION_HISTORY table 29
SYNCHRONIZATION_LOCK table 29
system configuration 154

T

T_AccessCatalog table 56
T_AccessCatalogTags table 57
T_AttributeEntitlement table 61
T_BADGES table 58
T_Global_Settings table 63
T_GROUP table 58
T_GROUP_PROFILE table 63
T_Joindirective table 63
T_Owner table 58
T_PolicyMembership table 60
T_ProvisioningPolicy table 59
T_Role table 59
T_ServiceEntitlement table 60
T_ServiceTags table 61
TASK_TREE table 79
TASKS_VIEWABLE table 79
TMP_HostSEByPerson table 62
TMP_JSAEByPerson table 62

U

user audit
namespace 221
query items 222
query subjects 221
user configuration
namespace 225
query items 226
query subjects 225
USERRECERT_ACCOUNT table 41
USERRECERT_GROUP table 42
USERRECERT_HISTORY table 40
USERRECERT_ROLE table 40

V

V_AUTHORIZED_CREDENTIALPOOLS view 54
V_AUTHORIZED_CREDENTIALS view 54
V_DYNAMIC_ENTITLEMENT view 66
V_GC_CUSTOM view 69
V_GC_INTERSECT view 67
V_GROUP_PROFILE view 67
V_GroupCatalog view 63, 64
V_SA_EVALUATION_SERVICE view 55
V_SAPOLICY_ENTITLEMENT_DETAIL view 55
V_ServiceCatalog view 65
V_ServiceEntitlementByRole view 66
VIEW_DEFINITION table 79

W

WI_PARTICIPANT table 12
workflow tables 1
WORKFLOW_CALLBACK table 14
WORKITEM table 10

Printed in USA