IBM Security Identity Manager
Version 7.0.0.2

Administration Topics

IBM Security Identity Manager
Version 7.0.0.2

Administration Topics

Table of contents

Table list vii

Chapter 1. Virtual appliance management. 1

Appliance Dashboard 1
- Viewing the Disk Usage widget 1
- Viewing the Partition Information widget. . . . 1
- Viewing IP addresses 2
- Viewing the Notifications widget 2
- Viewing the Quick Links widget. 3
- Viewing the Server Control widget 3
- Viewing the Middleware Monitor widget. . . . 3
- Viewing the Cluster Status widget 4

Manage system settings for the virtual appliance . . 5
- Managing the update history information. . . . 5
- Managing the licensing and performance 6
- Managing the firmware settings 6
- Installing a fix pack 7
- Managing the About page information. 7
- Managing the memory usage 8
- Managing the CPU usage 9
- Managing the storage usage 10
- Monitoring the IBM Security Identity Manager Server 10
- Viewing the event log 13
- Managing the SNMP monitoring 14
- Managing the application interfaces 15
- Managing hosts file. 18
- Configuring static routes 19
- Managing the date and time settings 20
- Managing the administrator settings 21
- Managing the snapshots 21
- Managing the support files 23
- Configuring system audit events 24
- Restarting or shutting down 28

Chapter 2. User administration 29

User management 29
- Creating user profiles 30
- Changing user profiles 32
- Deleting user profiles 33
- Transferring users 34
- Suspending users 34
- Restoring users 35
- Recertifying users 36

Account management 37
- Requesting an account for a user 38
- Viewing accounts for a user 39
- Viewing or changing account details 40
- Deleting user accounts. 40
- Suspending user accounts 41
- Restoring user accounts 42

Access management 43
- Requesting access for users 44
- Viewing access for users 45
- Deleting user access 45

Password management 46
- Changing user passwords 46
- Resetting user passwords. 47
- Changing user passwords for sponsored accounts 48
- Resetting user passwords for sponsored accounts 49

Delegate activities 50
- Delegating activities for another user 51

Chapter 3. Login administration 53

Enabling password expiration 53
Setting a maximum number of login attempts . . . 53

Chapter 4. Password administration . . 55

Enabling password resetting. 55
- Hiding generated reset passwords. 56
- Showing generated reset passwords 56

Enabling password editing and changing 57
Enabling password synchronization 58
Setting a password when a user is created 59
Setting a password retrieval expiration 60
Setting password notification 60
Creating password strength rules 61
Enabling forgotten password authentication . . . 62
- Configuring administrator-defined forgotten password questions. 62

Excluding specific passwords 63
Passwords for system users 64
- Changing the itimuser user password 64
- Changing the db2admin user password for Windows 65
- Changing the ldapdb2 user password 66

Chapter 5. Organization administration 67

Administrator domains 67
Making a user a domain administrator 68
Creating a node in an organization tree 68
Changing a node in an organization tree 69
Deleting a node in an organization tree 69

Chapter 6. Security administration . . . 71

View management 71
- Creating a view 71
- Changing a view 72
- Deleting a view 72
- Defining a custom task 73
- Changing a custom task 75
- Deleting a custom task 76

Access control item management 76
- Default access control items 77
- Creating an access control item 83
- Changing an access control item 84
- Deleting an access control item 85

Chapter 7. Role administration 87
Role overview 87
Role hierarchy change enforcement 88
Creating roles 88
Modifying roles 89
Values and formats for CSV access data (role) . . . 90
Exporting access data for a role. 91
Importing access data for a role 92
Classifying roles 93
Specifying owners of a role 94
Displaying a role-based access in the user interface 95
Role assignment attributes 96
Defining assignment attributes when creating a role 98
Defining assignment attributes for an existing role 99
Setting assignment attribute values to the user members of a role 100
Configuring access catalog information for a role. 101
Deleting roles 102
Managing users as members of a role 103
Adding users to membership of a role 104
Removing users from membership of a role . . . 105
Managing child roles 106
Adding child roles to a parent role 107
Removing child roles from a parent role 109
Creating an access type based on a role. 110

Chapter 8. Services administration 111
Service types 112
Service status 114
Creating services 115
Creating a service that has manual connection mode 117
Enabling connection mode 120
Creating manual services 121
Changing services 123
Changing connection mode from manual to automatic 124
Changing a manual service 125
Values and formats for CSV access data (service) 126
Exporting access data for a service 127
Importing access data for a service 128
Configuring access catalog information for a service. 129
Deleting services 130
Management of reconciliation schedules 131
Reconciling accounts immediately on a service 134
Creating a reconciliation schedule 135
Changing a reconciliation schedule 136
Deleting a reconciliation schedule 137
Configuring a manual service type to support groups 138
Reconciling accounts immediately on a service 138
Example comma-separated value (CSV) file . . 139
Management of accounts on a service 141
Displaying accounts on a service 142
Requesting accounts on a service 143
Changing accounts on a service 144
Deleting accounts from a service 145
Suspending accounts on a service 146
Restoring accounts on a service 147
Assigning an account to a user 149
Orphan accounts 150
Management of account defaults on a service . . 152
Adding account defaults to a service 153
Changing account defaults for a service . . . 154
Removing account defaults from a service. . . 156
Using global account defaults for the service type 157
Service tagging 158
Adding the tag attribute to the service template 158
Adding tags to the service 159
Policy enforcement 159
Configuring policy enforcement behavior . . . 162
Configuring compliance alert rules 164
Enforcing policies 165
Account recertification 166
Displaying account recertification status . . . 166
Recertifying accounts on a service 167
Management of groups or access on a service . . 168
Clearing access 170

Chapter 9. Group administration . . . 173
Creating groups 173
Viewing group membership 174
Adding members to groups 175
Removing members from groups 177
Modifying groups 178
Values and formats for CSV access data (group) 179
Exporting access data for a group 180
Importing access data for a group 181
Deleting groups 182
Defining access on a group 184
Configuring access catalog information for a group 185
Recertifying access on a group 187
Enabling automatic group membership 188

Chapter 10. Report administration . . 189
IBM Cognos reporting framework 190
IBM Cognos reporting framework overview . . 190
Prerequisites for IBM Cognos report server . . 192
Installation of IBM Cognos reporting components 193
Configuration of IBM Cognos reporting components 194
Importing the report package 195
Creating a data source 196
Enabling the drill-through for PDF format. . . 197
Security layer configuration around the data model and reports. 198
Globalization overview 204
Report models 205
Report descriptions and parameters 208
Query subjects and query items for the report models 218
References 299
Troubleshooting report problems 305
IBM Security Identity Manager console reports . . 308
Types of reports 308

Generating reports 311
Regular expression notation usage for searching 313
Report customization 313
Data synchronization 336
Data synchronization for reports 337
Incremental data synchronizer overview . . . 340
Utility for external report data synchronization 344
Access control items (ACI) for reports 346
ACI object filters used for reporting 347

Chapter 11. Policy administration . . . 349

Adoption policies 349
Creating an adoption policy 350
JavaScript examples for writing adoption policies 351
Changing an adoption policy 353
Deleting an adoption policy 354
Attribute matching 354
Account reconciliation and orphan accounts . . 355
Identity policies 355
Identities 356
Identity policy script example (advanced approach) 356
Creating an identity policy 358
Changing an identity policy 360
Deleting an identity policy 360
Password policies 361
Creating a password policy. 361
Adding targets to a password policy 362
Creating a password policy rule 363
Changing a password policy 364
Changing targets for a password policy . . . 364
Changing a password policy rule. 365
Deleting a password policy. 366
Customized password rules 366
Provisioning policies 371
Policy enforcement 372
Provisioning policy parameter enforcement rules 373
Creating a provisioning policy. 374
Changing a provisioning policy 375
Previewing a modified provisioning policy . . 376
Creating a draft of an existing provisioning policy 377
Committing a draft provisioning policy . . . 378
Deleting a provisioning policy. 378
Managing provisioning policies by role. . . . 379
Recertification policies 379
Recertification activities 383
Recertification message templates and schedule 383
Recertification policy results 385
Creating an account recertification policy . . . 386
Creating an access recertification policy . . . 388
Creating a user recertification policy. 389
Changing a recertification policy 390
Deleting a recertification policy 391
Recertification default notifications 392
Separation of duty policies 394
ACI operations for the separation of duty policy protection category 395
Default ACIs for the separation of duty policy 396
Separation of duty approval workflow operation 396
Separation of duty policy violations and exemptions 397
Enabling the Manage Separation of Duty Policies portfolio task. 399
Creating separation of duty policies 400
Modifying separation of duty policies 401
Evaluating separation of duty policies 402
Deleting separation of duty policies 403
Viewing policy violations and exemptions. . . 404
Approving policy violations 405
Revoking policy exemptions 406
Service selection policies. 408
Creating a service selection policy 408
Changing a service selection policy 409
Deleting a service selection policy 410

Chapter 12. Workflow management 411

Adding an entitlement workflow 411
Changing an entitlement workflow 412
Deleting an entitlement workflow 413
Creating a mail activity template with the workflow designer 413
Workflow notification properties 415
Configuring the workflow escalation period . . 416
Configuring the work item reminder interval and reminder content. 417
Enabling workflow notification 418
Disabling workflow notification 418
Changing a workflow notification template . . 418
Manually applying the email notification template changes for canceling a request . . . 419
Sample workflows. 420
Sample workflow: manager approval of accounts 420
Sample workflow: multiple approvals 421
Sample workflow: multiple approvals with loop processing 424
Sample workflow: RFI and subprocess 427
Sample workflow: approval loop 428
Sample workflow: mail activity 430
Sample workflow: sequential approval for user recertification with packaged approval node . . 431
Sample workflow: packaged approval combined with simple approval node 434
Sample workflow: access owner approval . . . 437

Chapter 13. Activity administration 441

Approval activities 441
Approval states. 442
Request for information activities. 442
Request for information (RFI) states 443
Work order activities 443
Work order states 443
Compliance alert activities 444
Recertification activities 444
To-do lists 445
Requests 445
Escalation 445
View activities 447
Viewing activities (to-do items) 447

Viewing activities for a user 448
Completing an approval activity 448
Completing a request for information activity 448
Completing a work order activity 449
Completing a recertification activity 449
Completing a compliance alert activity 449
Deferring policy compliance alerts 450
Locking an activity 451
Unlocking an activity. 451
Assigning activities to another user 452
Delegate activities 452
Creating a delegation schedule 453
Changing delegation schedules 453
Deleting delegation schedules 454

Chapter 14. Requests administration 455
Requests 455
Request states 455
Viewing all requests 457
Viewing pending requests of users 457
Viewing all requests of users 458
Viewing pending requests by service 459
Viewing all requests by service 460
Canceling pending requests 461

Index 463

Table list

1. Application monitoring actions 11
2. Application Interfaces action items 17
3. Static route actions 19
4. Default access control items 77
5. CSV fields and values 90
6. Part 1 of 2: Role access CSV file values, formats 91
7. Part 2 of 2: Role access CSV file values, formats 91
8. CSV fields and values. 126
9. Part 1 of 2: Service access CSV file values, formats 127
10. Part 2 of 2: Service access CSV file values, formats 127
11. Default compliance alert settings 162
12. CSV fields and values. 180
13. Part 1 of 2: Group access CSV file values, formats 180
14. Part 2 of 2: Group access CSV file values, formats 180
15. Software requirements for IBM Cognos report server 192
16. Installation and data synchronization process 193
17. Configure IBM Cognos reporting components 194
18. LDAP advanced mapping values 199
19. Recertification model namespaces 206
20. Accounts model namespaces 206
21. Provisioning model namespaces 206
22. Roles model namespaces 207
23. Separation of duty model namespaces 207
24. Access model namespaces 208
25. Reports and the namespaces 208
26. Subreports 209
27. Filters for access definition report 209
28. Filters for Account Status Report 210
29. Audit History subreports 210
30. Filters for access audit history report 211
31. Filters for account audit history report 212
32. Filters for Entitlements Report 212
33. Recertification Definition subreports 214
34. Filters for Recertification Definition Report 214
35. Filters for Separation of Duty Policy Definition Report 214
36. Filters for Separation of Duty Policy Violation Report 215
37. Filters for Services Report 215
38. User Access subreports 215
39. Filters for the User Access report - View by Access report type 216
40. Filters for the User Access report - View by User report type 216
41. Filters for User Recertification History Report 217
42. Query subjects in the `Recertification Audit` namespace for the recertification model . . . 218
43. Query items in the `Recertification Audit` namespace 220
44. Query subjects in the `Recertification Config` namespace 228
45. List of query items in the `Recertification Config` namespace 229
46. Query subjects in the `Account Audit` namespace 235
47. Query items in the `Account Audit` namespace 236
48. Query subjects in the `Account Configuration` namespace 239
49. Query items in the `Account Configuration` namespace 241
50. Query subjects in the `Provisioning Policy Audit` namespace 248
51. Query items in the `Provisioning Policy Audit` namespace 250
52. Query subjects in the `Provisioning Policy Config` namespace 252
53. Query items in the `Provisioning Policy Config` namespace 253
54. Query subjects in the `Role Audit` namespace 255
55. List of query items in the `Role Audit` namespace 256
56. Query subjects in the `Role Configuration` namespace 258
57. List of query items in the `Role Configuration` namespace 260
58. Query subjects in the `Separation of Duty Audit` namespace 266
59. Query items in the `Separation of Duty Audit` namespace 267
60. Query subjects in the `Separation of Duty Configuration` namespace 271
61. Query items in the `Separation of Duty Configuration` namespace 272
62. Query subjects in the `User Configuration` namespace 273
63. List of query items in the `User Configuration` namespace 274
64. Query subjects in the `Service Audit` namespace 281
65. List of query items in the `Service Audit` namespace 282
66. Query subjects in the `Access Audit(Deprecated)` namespace 285
67. List of query items in the `Access Audit(Deprecated)` namespace 286
68. Query subjects in the `Access Audit` namespace 290
69. List of query items in the `Access Audit` namespace 291
70. Query subjects in the `Access Configuration` namespace 294
71. List of query items in the `Access Configuration` namespace 295
72. Mapping the attributes and entities 299
73. Basic tasks to configure report model 301

74. Entities and Attributes 319
75. Filter conditions 319
76. Entities and attributes. 320
77. Filter conditions 321
78. Entities and attributes. 322
79. Filter conditions 323
80. User input values 327
81. User input filters 329
82. Specifying the location of the Java runtime environment 345
83. System attribute enforcement rules 373
84. Recertification policies and access control items 380
85. Node properties: Sample workflow for manager approval 421
86. Node properties: Sample workflow for multiple approvals. 422
87. Node properties: Sample workflow for multiple approvals with loop processing . . 425
88. Node properties: Sample workflow with an RFI and a subprocess 427
89. Node properties: Sample workflow with an approval loop 429
90. Node properties: sample workflow for packaged approvals 432
91. Link properties: sample workflow for packaged approvals 433
92. Sample workflow node properties: Simple approval for user recertification with packaged approval node. 434
93. Link properties: Simple approval for user recertification 436
94. Relevant Data 437
95. Node properties: Sample workflow for access request. 438
96. Descriptions of the states of approval activities 442
97. Descriptions of the states of RFIs 443
98. Descriptions of the states of work order requests 444
99. Descriptions of the states of requests 455

Chapter 1. Virtual appliance management

For the virtual appliance, connect to the IBM® Security Identity Manager virtual appliance console to manage the virtual appliance settings.

Appliance Dashboard

The **Appliance Dashboard** provides important status information, statistics, and quick links to the administrative consoles.

Viewing the Disk Usage widget

You can view the disk space status and remaining disk life information with the **Disk Usage** widget on the **Appliance Dashboard**.

Procedure

1. On the **Appliance Dashboard**, locate the **Disk Usage** widget. The disk usage statistics are displayed.

   Disk Space Pie Chart
   Information about used disk space and free disk space is visualized in the pie chart.

   Used space
   Displays how much space (in GB) is already used.

   Note: Most of the disk space is typically used by log files and trace files. To minimize the disk footprint, set the virtual appliance to store log and trace files on a remote server. You can also clear unused log and trace files on a periodic basis.

   Free space
   Displays how much space (in GB) is available.

   Total space
   How much space in total (in GB) is available to the virtual appliance.

   Note: The disk space in a hardware appliance is limited by the capacity of the hard disk drive it holds.
2. Optional: Click **Refresh** to display the recently updated data.

Viewing the Partition Information widget

You can view information about the active and backup partitions with the **Partition Information** widget on the **Appliance Dashboard**.

Procedure

1. On the **Appliance Dashboard**, locate the **Partition Information** widget. Details about the active and backup partition are displayed.

   Firmware version
   Displays the version information about the virtual appliance firmware. For example, `7.0`.

Installation date
Displays the date on which the virtual appliance firmware was installed. For example, `Dec 01, 2014 8:15:51 PM`.

Installation type
Displays the type of the virtual appliance firmware installation. For example, `ISO`.

Last boot
Displays the time when the virtual appliance was last booted. For example, `Dec 01, 2014 8:19:40 PM`.

2. Click **Firmware Settings** to go the page to modify settings of the firmware. See "Managing the firmware settings" on page 6.

Viewing IP addresses

You can view a categorized list of IP addresses that the virtual appliance is listening on with the **Interfaces** widget.

Procedure

1. On the **Appliance Dashboard**, locate the **Interfaces** widget. The **Interfaces** widget displays a categorized list of IP addresses in a table with the following columns:
   - **Type**
   - **Name**
   - **Address**
2. Optional: Click **Refresh** to display the recently updated data.

Viewing the Notifications widget

You can view warning information about potential problems and required actions on the **Notifications** widget on the **Appliance Dashboard**.

About this task

The **Notifications** widget refreshes automatically after every 2 minutes to display the most recent state or condition of the IBM Security Identity Manager virtual appliance.

Procedure

1. On the **Appliance Dashboard**, locate the **Notifications** widget. Warning messages about potential problems and expected actions can be displayed as follows:

   ```
   Security Identity Manager server restart required
   Appliance restart required
   Middleware components not configured
   The disk space utilization has exceeded the warning threshold.
   ```

2. Take appropriate actions as necessary. For example:

   If the following warning message is displayed, restart the IBM Security Identity Manager Server by using the option that is provided in the **Server Control** widget.

   ```
   Security Identity Manager server restart required
   ```

   If a message for the **Appliance Dashboard** restart is displayed, restart the virtual machine from the `vSphere` console. This condition occurs only if you did not restart after your first configuration.

3. Optional: Click **Refresh** to display the most recent state or condition of the IBM Security Identity Manager virtual appliance.

Viewing the Quick Links widget

You can view the quick links for accessing the administration console application.

Procedure

1. On the **Appliance Dashboard**, locate the **Quick Links** widget.
2. Click a quick link to work with the application that is based on your requirement. For example, click **Identity Service Center**.

   Note: The default user ID is `itim manager` and password is `secret`.

Viewing the Server Control widget

You can view the status and control different servers in the **Appliance Dashboard** by using the **Server Control** widget.

About this task

Procedure

1. On the **Appliance Dashboard**, locate the **Server Control** widget. The **Server name** column displays a list of all the servers. For example:
   - IBM Security Identity Manager server
   - IBM Security Directory Integrator server
   - Cluster Manager server
2. Select a server from the list.
3. Do one of the following actions:

   Start Click **Start** to start the selected server.

   Stop Click **Stop** to stop the selected server.

   Restart
   Click **Restart** to restart the selected server.

   The **Server status** column displays the status of each server as follows:

   Started
   Indicates that the server is started.

   Stopped
   Indicates that the server is stopped.
4. Optional: Click **Refresh** to display the recently updated data.

Viewing the Middleware Monitor widget

The health status of a server is determined by the state of the middleware and services. You can view the health status information with the **Middleware Monitor** dashboard widget.

Procedure

1. On the **Appliance Dashboard**, locate the **Middleware Monitor** widget.
   The widget displays the various middleware servers. For example:
   - Identity data store
   - Directory Server status

The **Middleware status** displays the status of a server as follows:

Started
Indicates that the server is started.

Stopped
Indicates that the server is stopped.

Not configured
Indicates that the server is not configured.

2. Optional: Click **Refresh** to display the recently updated data.

Viewing the Cluster Status widget

You can view a list of all the nodes in the cluster on the **Cluster Status** widget of the **Appliance Dashboard**.

About this task

You can view the **Cluster Status** widget only on a cluster node of the IBM Security Identity Manager virtual appliance.

The **Cluster Status** widget is displayed only when you are in a cluster setup. In stand-alone environment, the widget is not displayed.

Procedure

1. On the **Appliance Dashboard**, locate the **Cluster Status** widget.

   If the **Cluster Status** widget is not displayed on the **Appliance Dashboard**, select **Dashboard** > **Cluster Status** and click **Save**.

   The **Cluster Status** widget displays the following table columns:

   Host Name
   Displays the host name of a node in the cluster. Click the host name of a node to open the **Appliance Dashboard** in a separate web browser. A node with no link indicates that it is the same node that you are working from.

   Role Displays the role of the node in the cluster.

   `Primary`
   Indicates that the node is `Primary`.

   `Member` Indicates that the node is `Member`.

   Status Displays the status of the node in the cluster.

   `Available`
   It indicates that the node is available for your business requirement.

   `Not Available`
   It indicates that the node is not available for your business requirement.

   Note: If the status of a node is displayed as `Not Available`, you can still click the host name link to start the **Appliance Dashboard**.

   `Undetermined`
   It indicates that the status of the node cannot be determined.

Synchronization State
Displays the synchronization state for the node.

Not Connected
Displays when a member node cannot connect to a primary node or when a primary node cannot connect to the member node.

Not Synchronized
Displays when the member node is not synchronized with the primary node.

Synchronized
Displays when the member node is synchronized with the primary node.

Synchronizing
Displays when the member node is synchronizing with the primary node.

Not Applicable
Displays if the cluster node is a primary node because the primary node does not require any synchronization.

Note: If an error occurs, an error icon is displayed. Check the logs for more information. See Managing the log configuration.

2. Optional: Click the **Refresh** icon to display the recently updated data.

Manage system settings for the virtual appliance

For your virtual appliance, you can work with system settings such as the log management and configuration, licensing, update history, firmware settings, fix packs, snapshots, support files, and other settings.

To manage the configured virtual appliance, log on to the **Appliance Dashboard** at `https://isimva_hostname`. For example: `https://isimva1.jk.example.com`.

Managing the update history information

View the update history to see a which firmware and security content updates are downloaded, installed, or rolled back on the IBM Security Identity Manager virtual appliance.

About this task

After you install an update, the update package is deleted from the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Update History**. The Update History page is displayed.

   The update history information is displayed in a table with the following columns:

   - **Name**
   - **Action Taken**
   - **Status**

- **Version**
- **Release Date**

2. Optional: Click **Refresh** to display the recently updated data.

Managing the licensing and performance

View the service agreement that you accepted when you installed the IBM Security Identity Manager virtual appliance. You can also add a license module to manage the licensing and performance.

About this task

A service agreement defines the agreement and formal commitments about the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Licensing and Performance**. The Licensing and Performance page is displayed.
2. Click **View Service Agreement** to view the service agreement.
3. Optional: Click **Select license** to add a license. Browse to the location to search and select the license module.

Managing the firmware settings

The IBM Security Identity Manager virtual appliance has two partitions with separate firmware on each partition. Partitions are swapped during firmware updates so that you can roll back the firmware updates.

About this task

Either partition can be active on the IBM Security Identity Manager virtual appliance. In the factory-installed state, partition 1 is active and contains the firmware version of the current released product. When you apply a firmware update, the update is installed on partition 2 and your policies and settings are copied from partition 1 to partition 2. The IBM Security Identity Manager virtual appliance restarts the system by using partition 2, which is now the active partition.

Note: The IBM Security Identity Manager virtual appliance comes with identical firmware versions installed on both of the partitions so that you have a backup of the initial firmware configuration.

Tip: Avoid swapping partitions to restore configuration and policy settings. Use snapshots to back up and restore configuration and policy settings.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Firmware Settings**. The Firmware Settings page is displayed.
2. On the Firmware Settings page, do one or more of the following actions.

Option	Description
Edit	Select the partition and click **Edit** to revise the partition comment.

Option	Description
Create Backup	**Important:** Create a backup of your firmware only when you are installing a fix pack that is provided by IBM Customer Support. Fix packs are installed on the active partition and you might not be able to uninstall the fix pack. **Note:** The backup process can take several minutes to complete.
Set Active	Set a partition active when you want to use the firmware that is installed on that partition. For example, you might want to set a partition active to use firmware that does not contain a recently applied update or fix pack.

3. Click **Yes**. If you set a partition to active, the IBM Security Identity Manager virtual appliance restarts the system by using the newly activated partition.

Installing a fix pack

Install a fix pack on the IBM Security Identity Manager virtual appliance to address software maintenance updates for reliability and performance enhancements.

Before you begin

Restriction: You cannot uninstall a fix pack by using the local management interface. You must use the command-line interface to uninstall a fix pack.

Fix packs are applied to your active partition. You can manually create a backup of your active partition before you apply a fix pack so that you can roll back your changes.

About this task

If a fix pack is installed on your IBM Security Identity Manager virtual appliance, you can view information about who installed the fix pack, comments, patch size, and the installation date.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Fix Packs**. The Fix Packs page is displayed.
2. On the Fix Packs page, click **New**.
3. In the Add Fix Pack window, click **Browse for fix pack** to locate, select, and add the fix pack file. The Browse for fix pack table displays the fix pack details.
4. Click **Save Configuration** to install the fix pack.

Managing the About page information

View the About page to learn or manage about the IBM Security Identity Manager virtual appliance and its content.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Maintenance** > **About**.
2. View the product-specific information for the IBM Security Identity Manager virtual appliance.

Results

The following information is displayed in the About page:

```
Product Name: IBM Security Identity Manager
Product Version:      7.0.
Server Name:          fitva1.in.ibm.com
Installed Fix Packs:  None
Build number:         20141202-1328
Build Date and Time:  Dec 02, 2014 1:32:57 AM
```

The About page items are described as follows.

Product Name
Displays the name of product that you are using.

Product Version
Displays the version of product that you are using.

Server Name
Displays the server name.

Installed Fix Packs
Displays the last fix pack level that was installed for the version of the product that you are using.

Build number
Displays the current build number for the version of the product that you are using.

Build Date and Time
Displays the date and the exact time and the time zone on which the last build occurred.

What to do next

Read the IBM Security Identity Manager virtual appliance product information to determine how it can be useful in your work.

Managing the memory usage

View the memory graph to see the memory that is used by the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **Memory**. The System Memory Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.

Option	Description
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the legend area, select **Memory Used** to review the total used memory. The **Details** section displays these statistics:

   Total Indicates the total system memory.

   Used Indicates the system memory that is used.

   Free Indicates the system memory that is available.

   As of Indicates the current date, time, and the UTC identifier.

Managing the CPU usage

View the CPU graph to see the CPU that is used by the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **CPU**. The System CPU Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the legend area, select the following options to review the CPU data. The **Details** section displays these statistics:

   User CPU
   Indicates the CPU use by the user.

   System CPU
   Indicates the CPU use by the system.

   Idle CPU
   Indicates the idle use of the CPU.

   As of Indicates the current date, time, and the UTC identifier.

Managing the storage usage

View the storage graph to see the percentage of disk space that is used by the boot and root partitions of the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **Storage**. The Storage Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend area, select which partitions that you want to review. The **Details** section displays these statistics:

   Boot Indicates the boot partition. It displays the size, used, and available storage information in MB.

   Root Indicates the base file system, where the system user is root. It displays the size, used, and available storage information in MB.

Monitoring the IBM Security Identity Manager Server

Configure the IBM Security Identity Manager Server monitoring with IBM Tivoli® Monitoring to collect performance metrics and service statistics from the IBM Security Identity Manager over a time.

Before you begin

Make sure that IBM Tivoli Monitoring Version 6.2.3 is installed before you work with the IBM Security Identity Manager Server monitoring.

Make sure that the Universal Agent is installed with the product. It might be installed on a separate computer.

For more information, see http://www.ibm.com/support/knowledgecenter/SSTFXA_6.2.3.1/com.ibm.itm.doc_6.2.3fp1/itm623FP1_install118.htm%23installation.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Monitor** > **Monitoring** > **Application**.

2. On the IBM Security Identity Manager Server Monitoring page, do one of these actions.

Table 1. Application monitoring actions

Configure the IBM Security Identity Manager Server monitoring	1. Click **Configure**. 2. On the Confirm action window, click **Yes**. 3. On the IBM Security Identity Manager server monitoring configuration window, provide these details. **Identity Manager administrator ID** The ID for the Security Identity Manager administrator. For example, `itim manager`. **Identity Manager administrator password** The password for the Security Identity Manager administrator. For example, `secret`. **Universal Agent host name** The host name of the Universal Agent. For example, specify `isimhost.mycompany.com`. **Universal Agent port** The port of the Universal Agent. For example, `7500`. **Monitoring interval** The time interval between 2 performance updates of the IBM Security Identity Manager Server. For example, `120` seconds. **Monitoring metrics** Select the items that you want to monitor for the IBM Security Identity Manager Server. **Select all** Select this option to monitor all the metrics for the IBM Security Identity Manager Server. **Service summary** Select this option to monitor the service summary. This metric contains cumulative information about all the IBM Security Identity Manager services. It includes statistics such as the number of services that failed and recovered. It also contains useful information such as the number of active processed requests, and number of threads that did not process. **Service details** Select this option to monitor the service details. This metric contains information about individual IBM Security Identity Manager services. It includes similar information as the service summary for each individual service instance. **Service failures** Select this option to monitor the service failures. This metric contains information about individual services that did not succeed. It includes this information: • The service name that did not succeed. • The number of requests that are blocked. • The date and time the service first did not succeed. • The error message that describes the failure. **Workflow requests** Select this option to monitor workflow requests. This metric contains information about requests that are processed by the IBM Security Identity Manager workflow. It contains statistics such as the number of processes that started and finished. **JMS queues** Select this option to monitor the JMS queues. This metric contains the sizes of the IBM Security Identity Manager JMS queues. These queues are an indication of the current workload. **Process statistics** Select this option to monitor the process statistics. This metric contains statistics about the Java™ process that runs IBM Security Identity Manager, such as CPU usage, memory consumption, thread count, and garbage collection. The thread count and garbage collection statistics are not enabled by default in WebSphere® Application Server. To see these statistics, enable the Java virtual computer profiler data. For more information, see http://www.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.nd.doc/info/ae/ae/tprf_jvmpidata.html. 4. Click **Save Configuration**. 5. Restart the cluster manager server if the **Notifications** widget indicates you to do it. A record is created for the IBM Security Identity Manager Server monitoring.
Enable the IBM Security Identity Manager Server monitoring	1. Select the record that you configured for the IBM Security Identity Manager Server monitoring. 2. Click **Enable**. 3. On the Confirm action window, click **Yes**. 4. Restart the cluster manager server if the **Notifications** widget indicates you to do it.

Table 1. Application monitoring actions (continued)

Disable the IBM Security Identity Manager Server monitoring	1. Select the record that you configured for the IBM Security Identity Manager Server monitoring. 2. Click **Disable**. 3. Restart the cluster manager server if the **Notifications** widget indicates you to do it.
Reconfigure the IBM Security Identity Manager Server monitoring	1. Click **Reconfigure**. 2. On the Edit IBM Security Identity Manager server monitoring configuration window, provide these details. **Identity Manager administrator ID** The ID for the Security Identity Manager administrator. For example, `itim manager`. **Identity Manager administrator password** The password for the Security Identity Manager administrator. For example, `secret`. **Universal Agent host name** The host name of the Universal Agent. For example, specify `isimhost1.mycompany.com`. **Universal Agent port** The port of the Universal Agent. For example, `7500`. **Monitoring interval** The time interval between 2 performance updates of the IBM Security Identity Manager Server. For example, `180` seconds. **Monitoring metrics** Select the items that you want to monitor for the IBM Security Identity Manager Server. **Select all** Select this option to monitor all the metrics for the IBM Security Identity Manager Server. **Service summary** Select this option to monitor the service summary. This metric contains cumulative information about all the IBM Security Identity Manager services. It includes statistics such as the number of services that failed and recovered. It also contains useful information such as the number of active processed requests, and number of threads that did not process. **Service details** Select this option to monitor the service details. This metric contains information about individual IBM Security Identity Manager services. It includes similar information as the service summary for each individual service instance. **Service failures** Select this option to monitor the service failures. This metric contains information about individual services that did not succeed. It includes this information: • The service name that did not succeed. • The number of requests that are blocked. • The date and time the service first did not succeed. • The error message that describes the failure. **Workflow requests** Select this option to monitor workflow requests. This metric contains information about requests that are processed by the IBM Security Identity Manager workflow. It contains statistics such as the number of processes that started and finished. **JMS queues** Select this option to monitor the JMS queues. This metric contains the sizes of the IBM Security Identity Manager JMS queues. These queues are an indication of the current workload. **Process statistics** Select this option to monitor the process statistics. This metric contains statistics about the Java process that runs IBM Security Identity Manager, such as CPU usage, memory consumption, thread count, and garbage collection. The thread count and garbage collection statistics are not enabled by default in WebSphere Application Server. To see these statistics, enable the Java virtual computer profiler data. For more information, see http://www.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.nd.doc/info/ae/ae/tprf_jvmpidata.html. 3. Click **Save Configuration**.

Table 1. Application monitoring actions (continued)

Export the IBM Security Identity Manager Server monitoring	1. Select the record that you configured for the IBM Security Identity Manager Server monitoring. 2. Click **Export** to save the file on your local computer. 3. Import the `isim.mdl` file into IBM Tivoli Monitoring Universal Agent to define the syntax of the metrics that the monitor sends to the Universal Agent. 4. Transfer this file to the computer where IBM Tivoli Monitoring is running. 5. On the IBM Tivoli Monitoring computer, copy the `isim.mdl` file into the directory that contains the Universal Agent meta files. For example: `C:\IBM\ITM\TMAITM6\metafiles`. 6. Ensure that the IBM Tivoli Monitoring Server and the IBM Tivoli Monitoring Universal Agent are running. 7. Import the metafile by using one of the following examples: • Example 1: a. Open a command editor. b. Type the **`C:\IBM\ITM\bin\um_console -h ITM_HOME`** command to go to the Universal Agent prompt. c. Type the **`import C:\IBM\ITM\TMAITM6\metafiles\isim.mdl`** command. • Example 2: a. Open a command editor. b. Type the **`C:\IBM\ITM\TMAITM6> kumpcon import isim.mdl`** command.

Viewing the event log

System events are logged when the system settings are changed or when problems occur with the IBM Security Identity Manager virtual appliance. Use the Event Log page to view and to export system events on your network.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Logs** > **Event Log**. The Event Log page displays system events in the **System Events** tab.
2. From the **System Events** tab, do one of the following actions.
   - Click **Pause Live Streaming** to stop the live updating of the event log.
   - Click **Start Live Streaming** to resume live updating of the event log.
   - Filter the system events by completing the following steps:
     a. Click the **Filter** button to display the Filter window.
     b. From the **Column** list, select a column name to filter on it. The column names are as follows:
        – **Any Column**
        – **Priority**
        – **Event ID**
        – **Event Description**
        – **Time Occurred**

        Note: The virtual appliance does not return results for the **Time Occurred** column when you select **Any Column**. Select the **Time Occurred** column to filter values in that column.
     c. From the **Condition** list, select a filter condition. Available filter conditions vary depending on the tab that you selected in the event log. The possible filtering conditions include these options:
        – **contains**
        – **is**
        – **starts with**
        – **ends with**

- **before**
- **after**
- **range**

Note: You can also add a rule for filtering the system events.

d. In the **Value** field, specify a filter value.

e. Click **Filter**.

f. Click **Clear** to clear all the filter changes.

- Click **Export** to download the displayed event log data to a CSV file.

Note: The default file name is `export.csv`.

a. In the exported event log file, the **Time Occurred** column shows the time since Epoch (1 January 1970, 00:00:00 Universal time).

b. When you use the table filter on the **Priority** field, the values that can be filtered are in English only (`low`, `medium`, and `high`). This behavior is expected on all language versions of the virtual appliance.

Managing the SNMP monitoring

The current virtual appliance status can be monitored by using SNMP. This status shows an SNMP agent, which can be queried by any SNMP manager or monitoring tools that support SNMP to obtain the status of the running virtual appliance.

About this task

When configured, the SNMP agent listens on all management interfaces.

The SNMP Monitoring function can be used to monitor the virtual appliance in an IBM Tivoli Monitoring environment. To monitor a virtual appliance by using IBM Tivoli Monitoring, use the Agentless Monitoring for Linux OS agent. For more information about configuring the IBM Tivoli Monitoring environment and the Agentless Monitoring for Linux OS agent, see the IBM Knowledge Center.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **SNMP Monitoring**.
2. On the SNMP Monitoring page, click **Configure**.
3. In the Configure SNMP window, select the **SNMP Protocol** version that the agent must use. The choices are as follows.
   - **Disabled**
   - **SNMPv1/SNMPv2c**
   - **SNMPv3**
4. In the **Port** field, type the number that the SNMP agent must listen on. Alternatively, you can also change the port number with the range controller next to it.

   Note: The default port number is 161.
5. Do the steps when you select one of these SNMP protocol options.

   SNMPv1/SNMPv2c

   In the **Community** field, type the name of the community that the SNMP manager uses to authenticate with the SNMP agent.

SNMPv3

Configure the following options to describe the user that accesses the SNMP agent. See this table.

Option	Description
Security Level	The security level of the user.
Security User	Type the name of the user that accesses the SNMP agent.
Auth Protocol	From the **Auth Protocol** list, select the authentication protocol to use.
Auth Password	Type the password to use for authentication. The password must be minimum 8 characters in length.
Auth Password (Confirm)	Retype the authentication password to confirm.
Privacy Protocol	From the **Privacy Protocol** list, select the privacy protocol to use.
Privacy Password	Type the password to be used as a privacy passphrase. The password must be a minimum of 8 characters in length.
Privacy Password (Confirm)	Retype the privacy password to confirm.

6. Click **Save Configuration**.
7. Optional: To reconfigure an existing SNMP Monitoring configuration, do these steps:
   a. From the SNMP Monitoring table, select a record.
   b. Click **Reconfigure**.
   c. In the Reconfigure SNMP window, edit the details.
   d. Click **Save Configuration**.
8. Optional: To unconfigure an existing SNMP Monitoring configuration, do these steps:
   a. From the SNMP Monitoring table, select a record.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion.

Managing the application interfaces

Set up a separate application interface for IBM Security Identity Manager. To manage application interfaces, use the Application Interfaces page.

About this task

When you configure the application interfaces after you upgrade the virtual appliance in a cluster, an error might occur with an exception, which can be displayed as follows.

```
<Trace Level="MIN">
 <Time Millis="1432096507108"] 2015.05.20 10:05:07.108+05:30</Time>
 <Server Format="IP">localhost</Server>
 <ProductId>CTGIM</ProductId>
 <Component>com.ibm.itim.startup</Component>
 <ProductInstance]ISIMVa_APP_MEMBER[/ProductInstance]
 <LogText><![CDATA[Exception during background service start.]]></LogText>
 <Source FileName="com.ibm.itim.startup.ServiceManager" Method="startServices"/>
 <Thread>Thread-86</Thread>
 <Exception><![CDATA[com.ibm.itim.startup.ServiceException: Failed to start service: ReconcilerCleanup
```

```
at com.ibm.itim.startup.ServiceManager.startServices(ServiceManager.java:458)
at com.ibm.itim.startup.ServiceManager.run(ServiceManager.java:218)
at java.lang.Thread.run(Thread.java:784)
Caused by: com.ibm.itim.startup.ServiceException: CORBA NO_PERMISSION 0x0 No; nested exception is:
org.omg.CORBA.NO_PERMISSION: java.rmi.AccessException:  ; nested exception is:
com.ibm.websphere.csi.CSIAccessException: SECJ0053E: Authorization failed for
<realmname>/<system user> while invoking (Home)ITIM#wf_ejb.jar#wf_ejb.enroleejb.MessageSenderHome create::2
is not granted any of the required roles: ITIM_SYSTEM   vmcid: 0x0  minor code: 0  completed: No
at com.ibm.itim.startup.RemoteServicesTerminator.start(RemoteServicesTerminator.java:58)
at com.ibm.itim.startup.ServiceManager.startServices(ServiceManager.java:434)
```

To fix the error, do these steps.

1. Log on to the primary node virtual appliance.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Advanced Configuration** > **Update Property**.
3. On the Update Property page, select the **All Properties** tab.
4. In the left pane, select the **Identity server property files** tab.
5. Select the `enRole.properties` file.
6. In the right pane, select the `enRole.appServer.url` property name.
7. Click **Edit** to open the Update property window.
8. In the **Property value** field, replace the occurrence of every host name IP with the application interface of the corresponding node.
9. Click **Save Configuration**.
10. Synchronize the nodes in the cluster. For more information, see Synchronizing a member node with a primary node.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Network Settings** > **Application Interfaces**. The Application Interfaces page displays the **Interface** tab. The **Interface** tab displays a table with these column names.

   Type Indicates whether the type is **IPv4** or **IPv6**.

   Mode Indicates whether the mode is **Static** or **Auto**.

   Address
   Indicates the address of the application interface.

   Netmask/Prefix
   Indicates the netmask or prefix of the application interface.
2. On the Application Interfaces page, do one of these actions.

Table 2. Application Interfaces action items

Action	Button	Description
Create an application interface	**New**	**Note:** • You can create only 1 application interface. Use a unique application interface across the cluster. • Make sure that you configure the management interface and the application interface in the same subnet. 1. Click **New** to display the Add Address window. 2. Select **IPv4** or **IPv6** to indicate the type of address to add. **IPv4** **IPv4** defines each interface on a network uniquely. **IPv4** is a 32-bit numeric address, which is written in decimal as four sets of digits, which are separated by periods, with no spaces or consecutive periods. Each number can be 0 - 255. For example: `9.122.20.250`. **IPv6** **IPv6** improves the efficiency of routing and provides greater security. **IPv6** is a 128-bit IP address, which is written in hexadecimal and separated by colons. For example: `4ffe:1800:8484:3:220:f9ff:fe25:70cf` 3. Do one of these actions. • For **IPv4 Settings**, do these steps. a. Select a mode. **Static** **Static** manually configures the network information for a host. **Auto** **Auto** is DHCP-assigned, which generates IP addresses automatically. b. Type an address value in the **Address** field. c. Type a net mask value in the **NetMask** field. • For the **IPv6 settings**, do these steps. a. Type an address value in the **Address** field. b. Specify a prefix value in the **Prefix** field. 4. Click **Save**. 5. If any notifications are displayed in the **Notifications** widget, take appropriate actions as necessary. The application interface record is listed in the Interface table.

Table 2. Application Interfaces action items (continued)

Action	Button	Description
Edit an existing application interface	**Edit**	1. Select an existing application interface. 2. Click **Edit** to display the Edit Address window. 3. Do one of these actions. • For **IPv4 Settings**, do these steps. a. Select **Static** or **Auto**. b. Edit address value in the **Address** field. c. Edit net mask value in the **NetMask** field. • For the **IPv6 settings**, do these steps. a. Edit address value in the **Address** field. b. Edit prefix value in the **Prefix** field. 4. Click **Save**. 5. In the Confirm Action window, a message indicates that editing the application interface restarts the virtual appliance. 6. Click **Yes**. **Note:** When the virtual appliance restarts after you edit a primary node application interface, log on to the member node and synchronize it with the primary node. To synchronize the nodes, see Synchronizing a member node with a primary node.
Test a connection	**Test**	1. Click **Test** to display the Ping Server window. 2. In the **Server** field, enter the IP address or name of the server to test the connection with. 3. Click **Test**. A message indicates whether the test connection was successful or not.
Refresh the application interface data	**Refresh**	Click **Refresh** to display the most recent version of the data, including changes that were made to the data since it was last refreshed.

3. Click **Save Configuration**.

Managing hosts file

To manage hosts file with the virtual appliance, use the Manage Hosts File page.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings** > **Network Settings** > **Hosts File**. All current host records with their IP addresses and host names are displayed.
2. On the Manage Hosts File page, work with host records or host names.
   - Add a host record
     a. Select the root level **Host Records** entry or do not select any entries.
     b. Click **New**.
     c. On the Create Host record page, do these actions.

        Address
        Specify the IP address of the host record.

Host Name
Specify the host name of the host record.

d. Click **Save**.

- `Add a host name to a host record`
  a. Select a host record entry to add the host name to.
  b. Click **New**.
  c. On the Add Hostname to Host Record page, enter the host name.
  d. Click **Save**.
- `Remove a host record`
  a. Select a host record entry to delete.
  b. Click **Delete**.
  c. On the confirmation page, click **Yes** to confirm the deletion.
- `Remove a host name from a host record`
  a. Select host name entry to delete.
  b. Click **Delete**.
  c. On the confirmation page, click **Yes** to confirm the deletion.

  Note: If the removed host name is the only associated host name for the IP address, then the entire host record (the IP address and host name) is removed.
- `Refresh the data`

  Click **Refresh** to display the most recent version of the data since it was last refreshed.

Configuring static routes

Configure static routes to the paired protection interfaces on your virtual appliance to enable network routers to redirect users to block pages or authentication pages.

About this task

This task is only necessary for networks that contain an extra network segment between the user segment and the virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Network Settings** > **Routes**.
2. On the Static Routes page, complete one of these steps.

Table 3. Static route actions

Field	Action
IPv4 Default Gateway	1. Specify an address value. For example: `9.113.50.1`. 2. Click **Save**. **Note:** Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.

Table 3. Static route actions (continued)

Field	Action
IPv6 Default Gateway	1. Specify an address value. For example: `3001:0DB9:0000:0000:02AB:00FF:FE29:9C6A`. 2. Click **Save**. **Note:** Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.
New	1. Click **New** to create a route. 2. In the Add Route window, define values in these fields. • **Destination** • **Gateway** • **Metric** • **Interface or Segment** 3. Click **Save Configuration**.
Edit	1. Select an existing route. 2. Click **Edit** to change the settings. 3. In the Edit Route window, edit values in these fields. • **Destination** • **Gateway** • **Metric** • **Interface or Segment** 4. Click **Save Configuration**.
Delete	1. Select an existing route. 2. Click **Delete**. 3. Click **Yes** to confirm your action.

Results

The new and edited system routes are displayed in the **Currently active system routes** table.

Managing the date and time settings

Use the Date/Time page to configure the date, time, time zone, and NTP server information of the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Date/Time**. The Date/Time page is displayed.
2. Configure the following options on the Date/Time page.

Option	Description
Date	Specifies the day, month, and year for the IBM Security Identity Manager virtual appliance.
Time	Specifies the time for the IBM Security Identity Manager virtual appliance.

Option	Description
Time Zone	Specifies the time zone for the IBM Security Identity Manager virtual appliance.
NTP Server address	Select **Enable NTP** to list the NTP (NIST Internet Time Service) servers that the IBM Security Identity Manager virtual appliance uses. You can enter multiple NTP servers, which are separated by commas.

Note: You cannot set the **Time Zone** or **Date/Time** by using the system console. You can specify only NTP server addresses.

3. Click **Save Configuration**.
4. Optional: Click **Reset** to set the configuration again or differently.

Managing the administrator settings

Use the administrator settings to change the password that you use to access your IBM Security Identity Manager virtual appliance. Use the settings to also access the length of idle time that is granted to pass before your session times out.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Administrator Settings**. The Administrator Settings page is displayed.
2. On the Administrator Settings page, type your current password in the **Current Password** field.
3. Type your new password in the **New Password** field.
4. Type your new password in the **New Password Confirmation** field.
5. In the **Session Timeout** field, click the arrows to select the amount of time that you are allowed to be idle before you are automatically logged out.
6. Click **Save Configuration**.

Managing the snapshots

Use snapshots to restore prior configuration and policy settings to the IBM Security Identity Manager virtual appliance.

Before you begin

Ensure that these steps are done before you want to create or apply a snapshot from the Snapshots page.

1. From the **Server Control** widget on the **Appliance Dashboard** for the primary node, do these steps.
   a. Select **Cluster Manager server**.
   b. Click **Stop**.
2. From the **Server Control** widget on the **Appliance Dashboard** for the member node, do these steps.
   a. Select **Security Identity Manager server**.
   b. Click **Stop**.
   c. Select **Security Directory Integrator server**.
   d. Click **Stop**.

When you restore the primary node from the backup node, some user requests remain in pending state. For example, Request for Service Access. Therefore, when you restore a backup node as a primary node, do these steps.

1. Clear the **Service Integration Bus** tables from the database and commit the changes. For more information, see Step 3 in "Reconfiguring the data store connection".
2. Restart the database server that you are using, such as DB2® or Oracle.
3. Restart the primary node virtual appliance.
4. Restart the member node virtual appliance.

About this task

Snapshots are stored on the IBM Security Identity Manager virtual appliance. However, you can download the snapshots to an external drive in case of system failure.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Snapshots**. The Snapshots page is displayed.
2. On the Snapshots page, do one or more of the following actions.

Option	Description
New	To create a snapshot, do these steps: 1. Click **New**. 2. On the Add Snapshot window, specify helpful comments in the **Comments** field, so that the snapshot is easy to identify in the virtual appliance. 3. Click **Save Configuration**.
Edit	To edit the comment for a snapshot, do these steps: 1. Select a snapshot. 2. Click **Edit**. 3. On the Edit Snapshot window, edit the existing comment in the **Comments** field. 4. Click **Save Configuration**.
Delete	To delete snapshots, do these steps: 1. Select one or more snapshots. 2. Click **Delete**. 3. Click **Yes** to confirm.

Option	Description
Apply	To apply a snapshot, do these steps: 1. Select a snapshot. 2. Click **Apply**. 3. Click **Yes** to confirm. **Important:** • You can apply a snapshot of the primary node on the backup node only from the command-line interface. • You must apply the snapshot of the same node that you are working on. • If you revert a snapshot in a cluster, apply the same level snapshot on each node in the cluster. • If configuration or policy versions are newer than the firmware version, the settings are rejected. If the configuration and policy versions are older than the firmware version, the settings are moved to the current firmware version.
Download	To download snapshots, do these steps: 1. Select one or more snapshots. 2. Click **Download**. 3. Browse to the location where you want to save the snapshot. 4. Save the file. **Note:** If you download multiple snapshots, the snapshots are compressed into a `.zip` file.
Upload	To upload a snapshot, do these steps: 1. Click **Upload**. 2. In the Upload Snapshot window, click **Browse for Snapshot**. 3. Select the snapshot that you want to upload. The snapshot information is displayed in the Files to upload table. 4. In the **Comments** field, type a comment to describe the snapshot. 5. Click **Save Configuration**. **Note:** You can upload only 1 snapshot at a time.
Refresh	To display the most recent list of snapshots, click **Refresh**.

Managing the support files

IBM Customer Support uses support files to help you troubleshoot problems with the IBM Security Identity Manager virtual appliance. Support files contain all log files, temporary and intermediate files, and command output that is needed to diagnose customer support problems.

About this task

Support files might contain customer-identifiable information, such as IP addresses, host names, user names, and policy files. Support files do not contain confidential information, such as passwords, certificates, and keys. All files inside a support file contain text that can be inspected and censored by the customer.

The support file contents are stored in a `.zip` file.

Tip: You can create multiple support files to track an issue over time.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Support Files**. The Support Files page is displayed.
2. On the Support Files page, do one or more of the following actions.

Option	Description
New	To create a support file, do these steps: 1. Click **New**. 2. In the **Comments** field of the Create Support file window, type a comment to describe the support file. 3. Click **Save Configuration**. A new support file is created on the IBM Security Identity Manager virtual appliance.
Edit	To edit the comment for a support file, do these steps: 1. Select a support file. 2. Click **Edit**. 3. On the Edit Support file window, edit the existing comment in the **Comments** field. 4. Click **Save Configuration**.
Delete	To delete support files, do these steps: 1. Select one or more support files. 2. Click **Delete**. 3. Click **Yes** to confirm.
Download	To download support files, do these steps: 1. Select one or more support files. 2. Click **Download**. 3. Browse to the location where you want to save the support files. 4. Save the file. **Note:** If you download multiple support files, the files are compressed into a `.zip` file.

Configuring system audit events

Configure where you want the IBM Security Identity Manager virtual appliance to send notifications about changes to system settings and problems with the virtual appliance.

About this task

Available objects include system audit events that are predefined in the virtual appliance and any system audit event objects that you created.

Important: Predefined system audit event objects cannot be deleted from the virtual appliance because they contain all the events that take place on the virtual appliance eventually. When you create objects such as SNMP, email, or syslog, you can delete these created objects.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**. The System Audit Events page displays the Available Objects pane and the Added Objects pane.

2. In the System Audit Events page, complete one or more of the following tasks.
   - To create a system audit event object, click **New**.

     The following system audit event objects are listed:
     - SNMP
     - Email
     - Remote Syslog

     See these related topics to configure one or more of the following system audit event objects.
     - "Configuring SNMP objects"
     - "Configuring email objects" on page 26
     - "Configuring remote syslog objects" on page 27
     -
   - To receive notifications for problems with the system, select one or more system audit event objects from the Available Objects pane, and add or move them to the Added Objects pane.
   - To edit a system audit event object, complete the following steps:
     a. Select a system audit event object in the Added Objects pane.
     b. Click **Edit**.
     c. Change the values in these fields according to your requirement.
        - **Name**
        - **Total Event Storage Limit**
        - **NAP Events Allocation**
        - **IPS Events Allocation**
        - **System Events Allocation**
        - **Comment**
     d. Click **Save Configuration**.
3. Optional: To delete a system audit event object, do these steps.
   a. Select a system audit event object that you created.
   b. Click **Delete**.
   c. Click **Yes** to confirm.
4. Click **Save Configuration**.
5. Optional: Click **Reset** to revert to the last updated changes.

Configuring SNMP objects

Configure Simple Network Management Protocol (SNMP) objects to enable the IBM Security Identity Manager virtual appliance to send system audit events to an SNMP manager. The SNMP notifications identify certain values and send them to an SNMP manager.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**.
2. In the System Audit Events page, take one of the following actions.
   - Click **New** > **SNMP** to display the Add SNMP Object window.
   - Select an existing SNMP object and then click **Edit** to display the Edit SNMP Object window.
3. In the **General** tab, type a name for the object.
4. Select an **SNMP version** from the list.

- V1
- V2C
- V3

5. In the **SNMP Manager** field, type the IP address, host name, or fully qualified domain name (FQDN) of the SNMP manager.

   Note: The SNMP host must be accessible to the virtual appliance to send SNMP traps.
6. Type the port number that the SNMP manager monitors for notifications.

   Note: The default port number is 162.
7. Type a comment to describe the SNMP object.
8. For SNMP versions V1 or V2c, type the name of the community that is used to authenticate with the SNMP agent.
9. For SNMP version 3, configure the following options.

Option	Description
Name	Type the user name to be authenticated in the SNMP database.
Notification Type	On the **Notification Type** tab, complete these steps. 1. Select **Inform** or **Trap** in the **Notification Type** field. 2. Specify the **SNMP Timeout** in seconds. **Note:** Specifying a timeout value is not mandatory.
Authentication and Privacy	On the **Authentication and Privacy** tab, complete these steps. 1. From the **Enable Authentication** list, select **Enabled** to enable authentication. 2. In **Authentication Passphrase**, type the relevant passphrase. 3. From the **Authentication Type** list, select a type. 4. From the **Enable Privacy** list, select **Enabled** to enable privacy. 5. In **Privacy Passphrase**, type the relevant passphrase. 6. From the **Privacy Type** list, select a type.

10. Click **Save Configuration**.

What to do next

After you configure an SNMP object, add the object to the Added Objects pane on the System Audit Events page. Add it so that the virtual appliance initiates the response when specified events occur.

Configuring email objects

You can create email objects to send an email notification to specified users or to administrators when specified events occur on your network. You can also select the event parameters to include in the message so that important information about detected events is provided.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**.
2. In System Audit Events page, take one of the following actions.
   - Click **New** > **Email** to display the Add Email Object window.
   - Select an existing email object and then click **Edit** to display the Edit Email Object window.
3. Configure the following options.

Option	Description
Name	Specifies a meaningful name for the response. **Note:** This name displays when you select responses for events, so give the response a name that allows users to easily identify what they are selecting.
From	Specifies the email address that displays in the **From** field of the email.
To	Specifies the email address or group of addresses to receive the email. **Note:** Separate individual email addresses with a comma or semicolon.
SMTP Server	Specifies the fully qualified domain name or IP address of the mail server. **Note:** The SMTP server must be accessible to the virtual appliance to send email notifications.
SMTP Port	Specifies the custom port that is used to connect to the SMTP server. The default is 25.
Comment	Type a comment to identify the email object.

4. Click **Save**.

What to do next

After you configure an email object, add the object to the Added Objects pane on the System Audit Events page. Add it so that the virtual appliance initiates the response when specified events occur.

Configuring remote syslog objects

Configure remote syslog objects to enable the system to record system events in a remote log file.

About this task

If the connection to the remote syslog server drops, the virtual appliance generates a system audit event. If you are using TCP protocol, the virtual appliance writes the events to an auxiliary storage file. When the connection is restored, events that are stored in this file are sent to the remote syslog server. If the connection is not restored before the storage file size exceeds, any additional events are dropped. The virtual appliance generates another system audit event when the connection is reestablished.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**.
2. In the System Audit Events page, do one of the following steps.
   - Click **Remote Syslog** to display the Add Remote Syslog Object window.
   - Select an existing remote syslog object and then click **Edit** to display the Edit Remote Syslog Object window.
3. Configure the following options.

Option	Description
Name	Specifies a meaningful name for the response.
Remote Syslog Collector	Specifies the fully qualified domain name or IP address of the host on which you want to save the log. **Note:** The host must be accessible to the virtual appliance.
Remote Syslog Collector Port	Specifies the custom port that is used to connect to the syslog collector. The default is 514.
QRadar Format Enabled	Select this check box to enable the virtual appliance to send events in QRadar LEEF format instead of RFC5424 remote syslog format.
Comment	Type a comment to identify the remote syslog object.

4. Click **Save Configuration**.

What to do next

After you configure a remote syslog object, add the object to the Added Objects pane on the System Audit Events page. Add it so that the virtual appliance initiates the response when specified events occur.

Restarting or shutting down

Use the Restart or Shutdown page to restart or shut down the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Restart or Shut down**. The Restart or Shutdown page is displayed.
2. Do one of the following tasks.

Option	Description
Restart	Restarting the IBM Security Identity Manager virtual appliance takes it offline for several minutes.
Shut Down	Shutting down the IBM Security Identity Manager virtual appliance takes it offline and makes it inaccessible over the network until you restart it.

Chapter 2. User administration

You can manage people and their user accounts and access in IBM Security Identity Manager.

A *person* is an individual in the system that has a person record in one or more corporate directories. Because information about a person can exist in the system without a user account, the term *user* is often used to describe a person that has profile information in Security Identity Manager.

A user who has an Security Identity Manager service account is called a Security Identity Manager user. Some people might not require an Security Identity Manager service account. For example, external customers or business partners who require access to a specific managed resource might not require an Security Identity Manager account. However, they might be populated into the system as persons.

Use the Manage Users page for the following tasks:

- Create and delete profiles that define a person in the system
- Change a user's personal profile
- Suspend or restore a person
- Transfer a person to another business unit
- Request an access or account for a person
- Change or delete an access/account for a person
- Change or reset user account passwords
- Delegate activities to a Security Identity Manager user
- Recertify a user (Only system administrators can perform this task.)

User management

A *user* is an individual who uses IBM Security Identity Manager to manage their accounts. A person who has an Security Identity Manager account is a resource user. Users need different degrees of access to resources for their work. Some users must use a specific application, while other users must administer the system that links users to the resources that their work requires.

Person profiles

A *profile* is a set of attributes that describe a person within the system, such as the user name and contact information.

The specific information contained in the profile is defined by the system administrator.

Attributes

An *attribute* is a characteristic that describes an entity, such as a user, an account, or an account type.

For example, a user is an entity. Some of the attributes that make up a user entity are full name, home address, aliases, and telephone number. These attributes are presented in the user personal profile. Attribute values can be modified, added, and deleted.

An attribute can be specified in an attribute field, as a filter, during a search for an account or user. Several attributes for accounts and account types can be customized by your system administrator.

Aliases

An *alias* is an identity name for a user. A user can have multiple aliases to map to the various user IDs that the user has for accounts.

A user can have several aliases; for example, `GSmith`, `GWSmith`, and `SmithG`.

Roles

Organizational roles are a method of providing users with entitlements to managed resources. These roles determine which resources are provisioned for a user or set of users who share similar responsibilities.

If users are assigned to an organizational role, the managed resources available to that role then become available to those users. Those resources must be properly assigned to that role.

A role might be a child role of another organizational role, which then becomes a parent role. The child role inherits the permissions of the parent role. In addition, a role might be a child role of another organizational role in a provisioning policy. The child role also inherits the permissions of provisioning policy.

Security Identity Manager groups

A *group* is a collection of Security Identity Manager users. Security Identity Manager users can belong to one or more groups. Groups are used to control user access to functions and data in Security Identity Manager.

Some users might belong to default groups that Security Identity Manager provides. Your site might also create additional, customized groups. Each group references a user category, which has a related set of default permissions and operations, and views that the user can access.

Groups grant specific access to certain applications or other functions. For example, one group might have members that work directly with data in an accounting application. Another group might have members that provide help desk assistance.

Creating user profiles

You can create an IBM Security Identity Manager user profile for an individual who requires one.

Before you begin

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

If a new user requires a new business unit, create the business unit first. A business unit might be necessary.

Procedure

To create an Security Identity Manager user, complete these steps:

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, click **Create**.
3. On the Select User Type page, select the user type. To place the user under a different business unit than the default, click **Search** to search for and select a business unit. Then, click **Continue**.
4. On the Create User page, click each tab and specify the required information for the user. The number of tabs that are displayed and the information in each tab is determined by your system administrator.
   a. On the **Personal Information** tab, type information about the user in the fields. To assign a role for this user, click **Search** to search and select an organizational role. Then, click **Business Information**.
   b. On the **Business Information** tab, type information about the user in the fields. Then, click **Contact Information**.
   c. On the **Contact Information** tab, type information about the user in the fields. Then, click **Assignment Attributes**.
   d. On the **Assignment Attributes** tab, specify values for the role assignment attributes for the user that you are creating. You can specify values for attributes only if you assigned a role to this user, and the role or its parent role contains assignment attributes.

      Note: You cannot specify values in the following cases:
      - You did not assign a role.
      - You assigned a role, but either the role or its parent role does not have assignment attributes.

   e. Click **Continue**.
5. On the Create a New Password page, provide a password for the user.
6. Choose a time and date to schedule this operation. You can select **Immediate**, or you can specify an effective date and time.
7. Click **Submit**. The user is provisioned an Security Identity Manager account with the password that you provide.
8. On the Success page, click **Close**.
9. On the Select a User page, click **Refresh**. The new user is displayed in the **Users** table.

What to do next

You can now do other activities for the new user, such as requesting accounts and access.

"Defining assignment attributes when creating a role" on page 98
When creating a role, you can optionally define assignment attributes to be associated with the role.

"Defining assignment attributes for an existing role" on page 99
When modifying an existing role, you can optionally define assignment attributes to be associated with the role.

"Setting assignment attribute values to the user members of a role" on page 100
You can set assignment attribute values to the user members of a static organizational role if you defined assignment attributes in the role definition.

Changing user profiles

You can change information that is associated with a IBM Security Identity Manager user by updating the user profile.

Before you begin

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

Procedure

To change a user profile, complete these steps:

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose personal profile you want to change, and click **Change**.
3. On the Change User page, click each tab and specify the required information for the user. The tabs that are displayed and the information in each tab is determined by your system administrator.
   a. On the **Personal Information** tab, type information about the user in the fields. To assign a role for this user, click **Search** to search for and select an organizational role. Then, click **Business Information**.
   b. On the **Business Information** tab, type information about the user in the fields. Then, click **Contact Information**.
   c. On the **Contact Information** tab, type information about the user in the fields. Then, click **Assignment Attributes**.
   d. On the **Assignment Attributes** tab, specify values for the role assignment attributes for the user that you are creating. You can specify values for attributes only if you assigned a role to this user, and the role or its parent role contains assignment attributes.

      Note: You cannot specify values in the following cases:
      - You did not assign a role.
      - You assigned a role, but either the role or its parent role does not have assignment attributes.

   e. Click **Continue**.
4. When your changes are done, click **Submit Now** to save the changes, or click **Schedule Submission** to select a date and time to schedule the change.
5. On the Success page, click **Close**.
6. On the Select a User page, click **Close**.

"Defining assignment attributes when creating a role" on page 98
When creating a role, you can optionally define assignment attributes to be associated with the role.

"Defining assignment attributes for an existing role" on page 99
When modifying an existing role, you can optionally define assignment attributes to be associated with the role.

"Setting assignment attribute values to the user members of a role" on page 100
You can set assignment attribute values to the user members of a static organizational role if you defined assignment attributes in the role definition.

Deleting user profiles

You can delete an IBM Security Identity Manager user profile. This action affects all the accounts that are associated with the user.

Before you begin

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

About this task

When you delete a user, all the accounts that are associated with the user become orphan accounts. You can optionally choose to delete the individual accounts that are associated with the user.

To delete a user:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, select the check mark next to the name of the user you want to delete. You can select one or more users to delete.
   c. You might want to delete all of the individual accounts that are associated with the user that you select. Select the **Include individual accounts when suspending, restoring, or deleting users** check box.

      Note: Only the individual accounts that are associated with the user are deleted. Sponsored accounts associated with the user are orphaned. For the ITIM Service, both individual accounts and sponsored accounts associated with this user are deleted.
   d. Click **Delete**.
3. On the Confirm page, review the users and their accounts to be deleted. Optionally, select a date and time to do the request.
4. Click **Delete** to submit your request.
5. On the Success page, click **Close**.
6. On the Select a User page, click **Close**.

What to do next

Assign owners to orphaned accounts. See "Assigning an account to a user" on page 149. If an account is no longer needed, delete the account. See "Deleting accounts from a service" on page 145.

Transferring users

When a user moves to a different business unit within the company, you can transfer the user to another business unit.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, select the check mark next to the full name of the user you want to transfer. You can select one or more users to transfer.
   c. Click **Transfer**.
3. On the Business Unit page, complete the following steps:
   a. Type information about the business unit in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Business Units** table, click the radio button next to the business unit to which you want to transfer the user. Click **OK**.
4. On the Confirm page, review the users and their accounts. Optionally, select a date and time to do the request, and then click **Transfer** to submit your request.
5. On the Success page, click **Close**.
6. On the Select a User page, click **Close**.

Suspending users

When a user leaves the company and no longer needs access to IBM Security Identity Manager, you can suspend the system access that the user has.

Before you begin

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

About this task

To suspend a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, select the check mark next to the full name of the user you want to suspend. You can select one or more users to suspend.

c. To suspend all of the individual accounts that belong to the user that you selected, select the **Include individual accounts when suspending, restoring, or deleting users** check box.

   Note: Sponsored accounts are not affected. You might want to customize the suspend user operation to handle sponsored accounts. For example, have the operation transfer the sponsored accounts to the service owner or the manager of the user who is suspended.

d. Click **Suspend**.

3. On the Confirm page, review the users and their accounts to be suspended. Optionally select a date and time to do the request, and then click **Suspend** to submit your request.
4. On the Success page, click **Close**.
5. On the Select a User page, click **Close**.

Restoring users

When a user is suspended, all the associated user accounts become inactive. Restoring an inactive user returns the user accounts to an active state.

Before you begin

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

About this task

To restore a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. To restore all of the individual accounts that belong to the user that you selected, select the **Include individual accounts when suspending, restoring, or deleting users** check box.

      Note: Sponsored accounts associated with the user are not affected. A suspended sponsored account must be restored through the account table.

   c. In the **Users** table, click the icon (▸) next to the name of the user you want to restore.
   d. Click **Restore**.

      If a password is required to restore the individual accounts of the user, you are prompted to change the password.

      If password synchronization is enabled

      - Individual accounts use the existing synchronized password. You are not prompted to change the password for individual accounts.
      - If no synchronized password exists, you are prompted to change the password. The passwords for all the individual accounts associated with the user are changed to the new password.

If password synchronization is disabled

You are prompted to change the password. The passwords for all the listed individual accounts are changed to the new password. Individual accounts on services that do not require password change on user restore are not affected by the password change.

3. If you want to schedule your change request for a later date and time, select **Effective Date**.
   a. Click the calendar and clock icons to select a date and time.
   b. Click **Submit**.
4. On the Success page, click **Close**.
5. Click **Refresh** to verify that the user is returned to active status.

What to do next

View the accounts for the restored user to ensure that the account status is active. Perform additional user administration tasks on the Select a User page, or click **Close** to exit the page.

Recertifying users

You can select a recertification policy and run that policy for a specific user. Only user recertification policies that are enabled can be located and run.

Before you begin

Only system administrators can perform this task.

About this task

You might need to run a recertification policy for a specific user for one of the following reasons:

- The recertification status is erroneous or needs to be changed.
- It might be necessary to override the results of one particular recertification policy with another.

To recertify a user, complete these steps:

Procedure

1. From the navigation tree, click **Manage Users**. The Manage Users page is displayed.
2. On the Manage Users page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**. A list of users that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   b. In the **Users** table, click the icon (▸) next to the user that you want to recertify, and then click **Recertify**. The Select a Recertification Policy page is displayed.
3. On the Select a Recertification Policy page, complete these steps:
   a. Type information about the policy in the **Search information** field.

b. In the **Search by** field, specify whether to search for policy names or descriptions, and then click **Search**. A list of policies that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

c. In the **Recertification Policies** table, select the policy that you want to run, and then click **Run**. A confirmation page is displayed.

4. On the Confirm page, click **Run**.

Results

A Success page is displayed, indicating that you successfully submitted a request to recertify the user.

What to do next

On the Success page, click **Close**.

Account management

You can manage accounts for users in IBM Security Identity Manager.

Accounts

An *account* is the set of parameters for a managed resource that defines an identity, user profile, and credentials.

An account defines login information (your user ID and password, for example) and access to the specific resource with which it is associated.

In IBM Security Identity Manager, accounts are created on services, which represent the managed resources such as operating systems (UNIX), applications (Lotus Notes®), or other resources.

Accounts, when owned, are either individual or sponsored. Individual accounts are for use by a single owner and have an ownership type of Individual. Sponsored accounts are assigned to owners who are responsible for the accounts, but might not actually use them to access resources. Sponsored accounts can have various types of non-Individual ownership types. IBM Security Identity Manager supplies three ownership types for sponsored accounts Device, System, and Vendor. You can create additional ownership types for sponsored accounts by using the Configure System utility.

Accounts are either active or inactive. Accounts must be active to log in to the system. An account becomes inactive when it is suspended. For example, a request to recertify your account usage might be declined and the recertification action is *suspend*. Suspended accounts still exist, but they cannot be used to access the system. System administrators can restore and reactivate a suspended account if the account is not deleted.

Account types

An *account type* represents a managed resource, such as an operating system, a database application, or another application that IBM Security Identity Manager manages. For example, an account type might be a Lotus Notes application.

Users access these account types by receiving an account on the managed resource. Contact your system administrator for additional information about the account types that are available in your environment.

Requesting an account for a user

You can request an account for a user.

Before you begin

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

Before you can request an account on a service, you must create that service. You must also define appropriate Service ACIs to enable the non-administrative users to search the services on the Request an Account>Select a Service page.

About this task

To request an account for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user who you want to request an account for.
   c. Click **Request accounts**. The Select a Service page is displayed.
3. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field, select an option in the **Search by** field, select an attribute from the **Service type** list, and then click **Search**.

      Note: Service ACIs must be defined to enable the non-administrative users to search the services.
   b. In the **Services** table, select the service on which you want to request an account.
   c. Click **Continue**. The Select an Ownership Type page is displayed.
4. Select the ownership type for the account, and then click **Continue**. The number of ownership types is determined by the provisioning policy entitlements for the service. The default provisioning policy entitles accounts to the Individual ownership type. Any additional ownership types must be added to the provisioning policy for the service.

Note: If only one ownership type is entitled, this page is not displayed. All accounts are created with that ownership type. For example, if the default provisioning policy is used, all accounts are created as individual accounts. The User page is displayed.

5. On the User page, complete these steps:
   a. Click each tab and specify the required information for that account. The tabs that are displayed vary based on the type of service that you selected. For example, for the AIX® service, account information, access information, and administration information pages is displayed.
   b. If password editing is disabled, click **Submit Now** to complete the request, or click **Schedule Submission** to select a date and time to schedule the request.
   c. If password editing is enabled, click **Continue** to proceed to the Password page. Create a password for the account you are requesting. To specify a password for the account, select whether you want to have the system generate the password or to specify the password now. Click **Submit Now** to complete the request, or click **Schedule Submission** to select a date and time to schedule the request. If you specify a password, the password must conform to the password strength rules for the account.
6. On the Success page, click **Close**.
7. On the Manage Accounts page, click **Close**.

Viewing accounts for a user

You can view a list of accounts for users in IBM Security Identity Manager.

Before you begin

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

About this task

To view a list of accounts for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose accounts you want to view, and click **Accounts**.
3. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.
4. On the Accounts page, when you are done viewing accounts, click **Close**.

Viewing or changing account details

You can view or change account details for user accounts in IBM Security Identity Manager.

Before you begin

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

About this task

To view or change account details for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose accounts you want to view or change, and click **Accounts**.
3. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.
4. On the Accounts page, click the user ID to view or change account details.
5. On the Account Information page, view account details, or if you want to change account details, specify the required information for the user. The tabs that are displayed and the information in each tab is determined by your system administrator. When your changes are done, click **Submit Now** to save the changes, or click **Schedule Submission** to select a date and time to schedule the change.

   Note: When you change account information for the administrator account, such as ITIM Manager, there might be limitations on which information you can change. If the administrator account is configured to use an authentication repository other than ITIM service, you cannot force the account to change password at the next login. When the authentication repository is not ITIM Service, IBM Security Identity Manager does not manage the password.
6. On the Success page, click **Close**.
7. On the Accounts page, when you are done viewing accounts, click **Close**.

Deleting user accounts

You can delete accounts for users in IBM Security Identity Manager.

Before you begin

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

About this task

To delete user accounts, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose accounts you want to delete, and click **Accounts**.
3. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.
4. On the Accounts page, select the check mark next to any accounts you want to delete that are associated with a specific user ID and service name. You can select one or more user accounts to delete. Click **Delete**.
5. On the Confirm page, verify that you want to delete the listed accounts, optionally select a date and time to do the request, and then click **Delete**.
6. On the Success page, click **Close**.
7. On the Manage Accounts page, click **Close**.

Suspending user accounts

You can suspend user accounts in IBM Security Identity Manager. When you suspend an account, it becomes inactive.

Before you begin

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

About this task

To suspend user accounts, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.

b. In the **Users** table, click the icon (▸) next to the name of the user whose account you want to suspend, and click **Accounts**.

3. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.
4. On the Accounts page, select the accounts you want to suspend that are associated with a specific user ID and service name. You can select one or more user accounts to suspend. Click **Suspend**.
5. On the Suspend Accounts page, verify that you want to suspend the listed accounts. Optionally, select a date and time to do the request, and then click **Suspend**.
6. On the Success page, click **Close**.
7. On the Manage Accounts page, click **Close**.

Restoring user accounts

You can restore inactive user accounts that were suspended in IBM Security Identity Manager. When you restore an account, it becomes active again.

Before you begin

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

About this task

To restore a user account, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose account you want to restore, and click **Accounts**.
3. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.
4. On the Accounts page, select the check marks next to the accounts that you want to restore. The account is associated with a specific user ID and service name. Click **Restore**.

Note: If a password is required to restore the selected accounts, you are prompted to change the password for those accounts.

If password synchronization is enabled

- Individual accounts use the existing synchronized password. You are not prompted to change the password for individual accounts. If you are restoring sponsored accounts, you are prompted to change the password for those listed accounts. The passwords for all listed sponsored accounts are changed to the new password.
- If no synchronized password exists, you are prompted to change the passwords for all listed accounts regardless of ownership type. The passwords for all the listed accounts are changed to the new password. If you change the password of an individual account, the password change applies to all individual accounts. The passwords for individual accounts not listed are synchronized to the new password.

If password synchronization is disabled

You are prompted to change the password. The passwords for all listed accounts regardless of ownership type are changed to the new password.

5. On the Restore Accounts page, verify that you want to restore the listed account. Optionally select a date and time to do the request. Click **Submit**.
6. On the Success page, click **Close**.
7. On the Manage Accounts page, click **Close**.

What to do next

View the accounts of the user to ensure that the account is active.

Access management

You can manage access to resources for users in IBM Security Identity Manager. *Access* is your ability to use a specific resource, such as a shared folder or an application.

Access

In IBM Security Identity Manager, access can be created to represent access to access types such as shared folders, applications (such as Lotus Notes), email groups, or other managed resources.

An access differs from an account in that an account is a form of access; an account is access to the resource itself.

Access is the permission to use the resource. *Access entitlement* defines the condition that grants access to a user with a set of attribute values of a user's account on the managed resource. In IBM Security Identity Manager, an access is defined on an existing group on the managed service. In this case, the access is granted to a user by creating an account on the service and assigning the user to the group. Access entitlement can also be defined as a set of parameters on a service account that uses a provisioning policy.

When a user requests new access, by default an account is created on that service. If an account exists, the account is modified to fulfill the access entitlement. For example, you can assign the account to the group that grants access to an access

type. If one account exists, the account is associated with the access. If multiple accounts exist, you must select the user ID of the account to which you want to associate your access.

An access is often described in terms that can be easily understood by business users.

Requesting access for users

You can request access for a user. Access gives the user the ability to use a specific resource.

Before you begin

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

Before you can request access, you must create an access entitlement for a service.

About this task

Only access associated with entitlements of the ownership type Individual can be granted (request by users). If you request access for a user with a sponsored account, an individual account is automatically created. For example, you request access for a user whose preferred user ID is `jdoe`. The user account is a sponsored account with the ownership type Vendor. A user ID `jdoe1` is created with an individual account for the requested access.

To request access for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user who you want to request access for.
   c. Click **Request access** to display the Select Access page.
3. On the Select Access page, complete these steps:
   a. Type information about the service in the **Access information** field, select an access type from the **Access type** tree, and then click **Search**.
   b. In the **Access** table, select the access that you want to request.
   c. Click **Continue**.
4. On the Select Accounts page, select one or more accounts that you are requesting the access for. This page is displayed only if more than one individual account exists.
5. Click **Submit** to complete the request, or click **Schedule Submission** to select a date and time to schedule the request.
6. On the Success page, click **Close**.
7. On the Select Access page, click **Close**.

Viewing access for users

You can view access for a user.

Before you begin

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

About this task

To view access for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user for which you want to view access.
   c. Click **Access**.
3. When you are finished viewing access entitlements, on the Manage Access page, click **Close**.

Deleting user access

You can delete access for users in IBM Security Identity Manager.

Before you begin

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

About this task

To delete access for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose accounts you want to delete, and click **Access**.
3. On the Access page, select the check mark next to the access you want to delete that is associated with a specified access name. Click **Delete**.
4. On the Confirm page, verify that you want to delete the listed access, optionally select a date and time to do the request, and then click **Delete**.
5. On the Success page, click **Close**.
6. On the Access page, click **Close**.

Password management

There are two ways to manage passwords in IBM Security Identity Manager.

When password editing is enabled, you can supply user passwords with the **Change Passwords** task. When password editing is disabled, you can reset user passwords with the **Reset Passwords** task.

Changing user passwords

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

Before you begin

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

About this task

If password editing is disabled, you must use the **Reset Passwords** option to modify passwords because you do not have access to the **Change Passwords** task.

If password synchronization is enabled, the password is changed for all of the individual accounts automatically.

If password synchronization is not enabled, you can choose which accounts you want to change the password for.

Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.

To change passwords for other users, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user for whom you are changing passwords in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose passwords you want to change, and click **Change Passwords**.
3. On the Change Passwords page, complete these steps:
   a. Select how you want the password to be generated. If you select to type a new password, type and confirm the password.
   b. Select the accounts that you want to change the password for.

      Note: If password synchronization is enabled and you are changing the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to the maximum search limit. These accounts are not selectable. The password change applies to all individual accounts. The individual accounts that are not listed are also changed.

c. If you want to schedule your change request for a later date and time, click the icon (▸) next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.

d. Click **Submit**.

4. On the Success page, click **Close**.

"Resetting user passwords"
When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

"Changing user passwords for sponsored accounts" on page 48
When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

"Resetting user passwords for sponsored accounts" on page 49
When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Resetting user passwords

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Before you begin

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

About this task

If password editing is enabled, you must use the **Change Passwords** option to modify passwords because you do not have access to the **Reset Passwords** task.

If password synchronization is enabled, the password is changed for all of the individual accounts automatically.

If password synchronization is not enabled, you can choose which accounts you want to change the password for.

Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.

To reset passwords for other users, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user for whom you are resetting passwords in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose passwords you want to reset, and click **Change Passwords**.
3. On the Reset Passwords page, complete these steps:
   a. Select the accounts that you want to reset the password for.

Note: If password synchronization is enabled and you are resetting the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to the maximum search limit. These accounts are not selectable. The password reset applies to all individual accounts. The individual accounts not listed are also changed.

b. If you want to schedule your change request for a later date and time, click the icon (▸) next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.

c. Click **Submit**.

4. On the Success page, click **Close**.

"Changing user passwords" on page 46
When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

"Changing user passwords for sponsored accounts"
When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

"Resetting user passwords for sponsored accounts" on page 49
When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Changing user passwords for sponsored accounts

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

Before you begin

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

About this task

If password editing is disabled, you must use the **Reset Passwords** option to modify passwords because you do not have access to the **Change Passwords** task.

Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.

To change passwords for other users, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user for whom you are changing passwords in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click (▸) next to the name of the user whose passwords you want to change, and click **Accounts**.
   c. On the Accounts page, type information about the account that you are changing password for in the **Search information** field. Select an attribute from the **Search by** list, and select an ownership type. Click **Search**.

d. Click (▸) next to the name of the account, and click **Change Password**.

3. On the Change Passwords page, complete these steps:
   a. Select how you want the password to be generated. If you select to type a new password, type and confirm the password.
   b. Select the accounts that you want to change the password for.

      Note: If password synchronization is enabled and you are changing the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to the maximum search limit. These accounts are not selectable. The password change applies to all individual accounts. The individual accounts not listed are also changed.
   c. If you want to schedule your change request for a later date and time, click the icon (▸) next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.
   d. Click **Submit**.
4. On the Success page, click **Close**.

"Resetting user passwords for sponsored accounts"
When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

"Changing user passwords" on page 46
When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

"Resetting user passwords" on page 47
When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Resetting user passwords for sponsored accounts

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Before you begin

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

About this task

If password editing is enabled, you must use the **Change Passwords** option to modify passwords because you do not have access to the **Reset Passwords** task.

Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user for whom you are resetting passwords in the **Search information** field. Select an attribute from the **Search by** list, and then click **Search**.

b. In the **Users** table, click (▸) next to the name of the user whose passwords you want to change, and click **Accounts**.
c. On the Accounts page, type information about the account that you are changing password for in the **Search information** field. Select an attribute from the **Search by** list, and select an ownership type. Click **Search**.
d. Click (▸) next to the name of the account, and click **Reset Password**.

3. On the Reset Passwords page, complete these steps:
   a. Select the accounts that you want to reset the password for.

      Note: If password synchronization is enabled and you are resetting the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to the maximum search limit. These accounts are not selectable. The password reset applies to all individual accounts. The individual accounts that are not listed are also changed.
   b. If you want to schedule your change request for a later date and time, click the icon (▸) next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.
   c. Click **Submit**.
4. On the Success page, click **Close**.

"Changing user passwords for sponsored accounts" on page 48
When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

"Changing user passwords" on page 46
When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

"Resetting user passwords" on page 47
When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Delegate activities

You can delegate activities to another user during a time when other users are not available to manage them.

To delegate activities from one user to another user, the user you are delegating to must have authorization from the system administrator to manage activities. If you are delegating activities for yourself, you must have both read and write Delegate access control item attribute permissions set to `Grant`. The logged-in user must have the access control item permission to write the `delegate` attribute of the user who is delegated.

You can add or delete delegation schedules for the user whose activities you are delegating. Adding a delegation schedule requires you to select a user who can manage activities and specify a time period in which to delegate activities. You can set up multiple delegation schedules for multiple delegates, but time periods cannot overlap. If you already delegated activities and want to turn off delegation, delete the delegation schedule.

Delegation does not affect the escalation period for an activity; that is, it does not restart the countdown to the escalation date.

Delegating activities for another user

When a user is unavailable to manage activities, you can create a delegation schedule to delegate the to-do items of that user to another user.

Before you begin

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

About this task

To delegate activities, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, complete these steps:
   a. Type information about the user for whom you are delegating activities in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
   b. In the **Users** table, click the icon (▸) next to the name of the user whose accounts you want to delegate, and click **Delegate Activities**.
3. On the Manage Delegation Schedules page, click **Add** to create a delegation schedule.
4. On the Setup Delegation page, click **Search** to find a delegate.
5. On the Select Delegate Account page, complete these steps:
   a. Type information about the delegate in the **User ID** field and click **Search**.
   b. In the **Accounts** table, select the user whose account you want to delegate your activities to, and click **OK**.
6. On the Setup Delegation page, click the calendar and clock icons to choose a date and time for starting and ending the delegation, and click **OK**.
7. On the Success page, click **Close**.

Chapter 3. Login administration

You can configure system login settings to control the interval at which the password of an account expires. You can configure the number of times that a user can attempt to log in before the account is suspended.

Enabling password expiration

You can configure password settings to force users to regularly change their IBM Security Identity Manager passwords within a specified time period.

Before you begin

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

Note: If you configured IBM Security Identity Manager to use the default custom registry, you can enable password expiration. If you configured IBM Security Identity Manager to use an external user registry for authentication, you cannot enable password expiration.

Users who are forced to change their password because of an expired password period are taken to the Expired Password page immediately after login. The user cannot access any features in the system until the password is changed.

About this task

To enable password expiration, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. In the **Identity account password expiration period in days** field, type a time period, and then click **OK**. The default value of 0 indicates that the account password never expires.
3. On the Success page, click **Close**.

Setting a maximum number of login attempts

You can set a limit on the number of unsuccessful login attempts that a user can make. You can also suspend accounts that exceed a specified maximum number of login attempts. After the user account is suspended, the user must contact you (the system administrator) or a help desk representative. You can then restore the account and generate or provide a new temporary password for the user.

Before you begin

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

This task is available only for administrators and cannot be customized.

About this task

This task applies only if the ITIM Service user registry is used. If another user registry is specified, the number of login attempts is managed by the external repository.

The login attempts setting also applies to incorrect challenge response answers.

To set a maximum number of login attempts, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. In the **Maximum number of incorrect login attempts**, type the number of login attempts you want to allow, and then click **OK**. The default value of 0 indicates that there is no limit to the number of entries that can be attempted.
3. On the Success page, click **Close**.

Chapter 4. Password administration

IBM Security Identity Manager controls how passwords can be changed, generated, synchronized, and set throughout the system.

Tasks for managing system-wide password settings include:

- Enabling password resetting, including:
  - Hiding generated passwords from the administrators who generate them
  - Showing generated passwords to the administrators who generate them
- Enabling editing and changing passwords
- Synchronizing password changes for all of the individual accounts that are associated with a user
- Setting passwords when the user is created
- Setting an interval in which a user must retrieve a password before it expires
- Creating a password strength rule
- Enabling forgotten password authentication
- Excluding specific passwords

Password expiration settings are part of the login account settings.

Depending on the adapters that are used in your site environment, you might optionally set reverse password synchronization. The synchronization originates from a master password store other than IBM Security Identity Manager.

A help desk assistant can also request IBM Security Identity Manager to generate a password. The password is sent in an email to the user.

For information about managing user passwords, including the passwords of system users, see "User management" on page 29.

Enabling password resetting

Users or administrators with the correct permissions can *reset* users' passwords to new passwords that are generated by IBM Security Identity Manager. Alternatively, depending on the password settings of Security Identity Manager, users or administrators might be able to *change* users' passwords to new passwords. The new passwords must be manually specified within the limits of the password policy.

Before you begin

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

About this task

To reset another user's passwords, you must have the correct access control item permissions.

You must configure your system to use either the **Reset Passwords** function or the **Change Passwords** function. The options are not available at the same time.

If you choose to enable the **Reset Passwords** function, you also have the option of showing or hiding the generated password.

To enable password resetting:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. Clear the **Enable password editing** check box, and click **OK**.
3. On the Success page, click **Close**.

Hiding generated reset passwords

You might want to prevent every user or administrator who can reset passwords from seeing the new password that is generated. You can disable password editing and hide generated passwords.

Before you begin

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

About this task

If you do not hide generated passwords, the users or administrators who are resetting a user's password see the password that was generated.

To enable **Reset Passwords** and hide the generated password from the user or administrator who requested that the password be reset, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. Select the **Hide generated passwords for others** check box, and click **OK**.

   Note: If the **Enable password editing** check box is selected, you cannot select the **Hide generated passwords for others** check box. Clear the **Enable password editing** check box if you want to hide generated passwords.
3. On the Success page, click **Close**.

Results

A group member who can create accounts, such as a member of the help desk assistant group, can reset a password. However, the group member cannot see the new password. IBM Security Identity Manager generates the password.

Showing generated reset passwords

You might want to enable every user or administrator who can reset passwords to see the new password that is generated. You can disable password editing and clear the hide generated passwords check box.

Before you begin

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

About this task

If you do not hide generated passwords, the users or administrators who are resetting a user's password see the password that was generated.

To enable the **Reset Passwords** and show the generated password to the user or administrator who requested that the password be reset, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. Ensure that the following conditions are true:
   - The **Enable password editing** check box is not selected.
   - The **Hide generated passwords for others** check box is not selected.
3. Click **OK**.
4. On the Success page, click **Close**.

Results

A group member who can create accounts, such as a member of the help desk assistant group, can reset a password. The group member can also see the new password.

Enabling password editing and changing

Users or administrators with the correct permissions can *reset* users' passwords to new passwords that are generated by IBM Security Identity Manager. Alternatively, depending on the password settings of Security Identity Manager, users or administrators might be able to *change* users' passwords to new passwords. The new passwords are manually specified within the limits of the password policy.

Before you begin

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

About this task

To change another user's passwords, a user or administrator must have the correct access control item permissions. When you enable password editing, the user or administrator with the correct access control permissions can manually specify the password.

You must configure your system to use either the **Reset Passwords** function or the **Change Passwords** function. The options are not available at the same time.

To enable password editing, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. Select the **Enable password editing** check box, and click **OK**.
3. On the Success page, click **Close**.

Results

Enabling password editing has these results:

- Disables the ability to hide generated passwords for others.
- Enables users with the correct authority to select the **Change Passwords** option in the navigation tree and then change their own passwords.
- Enables a group member who can create accounts to create and set a value for a password for an account of another user. For example, the group member might belong to the help desk assistant group. Because the newly created password is visible, the help desk assistant can provide the information by telephone to the user.

What to do next

Note: You must log out and log back in to see the changes that are made to the navigation tree after you enable password editing.

Enabling password synchronization

Password synchronization is the process of assigning and maintaining one password for all individual accounts that a user owns. Password synchronization reduces the number of passwords that a user must remember. Password synchronization does not affect sponsored accounts.

Before you begin

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

You must be a system administrator on the to enable password synchronization.

About this task

You can configure the system to automatically synchronize passwords for all individual accounts that are owned by a user. Then, the user must remember only one password. For example, a user might have two individual accounts: a IBM Security Identity Manager account and a Lotus Notes account. If the user changes or resets the password for the Security Identity Manager account, the Lotus Notes password is automatically changed to the same password as the Security Identity Manager password.

Note: When password synchronization is enabled, Security Identity Manager does the ACI evaluation for changing password on the person entity. (Before Tivoli Identity Manager version 5.0, the ACI evaluation was done on the account entity.) If the person ACI grants the user the change password operation, the user can change the password for all associated individual accounts. For sponsored accounts or if password synchronization is not enabled, the ACI evaluation is done against the account entity instead.

If password synchronization is enabled, users cannot specify different passwords for their individual accounts. Password synchronization does not affect sponsored accounts. A user can specify different passwords for sponsored accounts.

Note: When password synchronization is initially enabled, individual accounts of users are not automatically synchronized immediately. Accounts are synchronized when users change passwords or create an account.

To enable password synchronization, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. Select the **Enable password synchronization** check box, and click **OK**.
3. On the Success page, click **Close**.

What to do next

You can change and synchronize the passwords for the individual accounts that are associated with a user.

Setting a password when a user is created

You can enable a password to be generated and set for a user automatically at the time the user is created.

Before you begin

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

For the collected password to be set to auto-provisioned accounts, the following criteria must be met:

- An automatic entitlement that entitles the user to the account must exist.
- An account default for `erpassword` must exist at the service or service type level.

About this task

This option is intended to enable prompting for a password when creating users through the user interface. By default, IBM Security Identity Manager satisfies these criteria for IBM Security Identity Manager Server login accounts. A user that is created through the user interface is automatically provisioned an Security Identity Manager Server account with a known password. The password is entered at the time of user creation.

The system property for setting the password on a user during the user creation is configured for use during auto-provisioning of Security Identity Manager accounts only. When enabled, the "Set password on user..." system property gathers a password during user creation and stores it in the user record.

Also provided is an account default for the `ITIM Service` service type that sets `erpassword` during auto-provisioning to the value stored in the person record. You can configure another service to use this property by enabling the service for auto-provisioning and adding the necessary account default. Use the following account default script:

```
subject.getAndDecryptPersonPassword();
```

Note: If auto-provisioning is disabled, or if the account default is removed, disable the **Set password on user during user creation** property.

Procedure

To enable a password to be generated and set for a user at the time the user is created, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. Select the **Set password on user during user creation** check box, and click **OK**.
3. On the Success page, click **Close**.

Setting a password retrieval expiration

You can set a time by which a user must retrieve a password before it expires.

Before you begin

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

About this task

Password retrieval expiration specifies the time in which a user must retrieve a password. After the new account is created, the user receives an email with the URL link that provides the password. The user must get the password before this password retrieval period expires.

This password retrieval expiration property is in effect only when password retrieval is enabled.

Note: The shared secret attribute of Person and the notifyPassword property from `enRole.properties` file can be used for secured password retrieval.

To set a password retrieval expiration interval, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. Specify an expiration period in hours in the **Password retrieval expiration period in hours** field, and click **OK**.
3. On the Success page, click **Close**.

Setting password notification

As an administrator you can choose how to send password notifications to users for their accounts.

Before you begin

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

About this task

After creating an account, changing or resetting a password, you can specify how the password notification is sent to the user.

Procedure

1. Obtain the email address of the owner.
2. Set the value of the **enrole.workflow.notifypassword** property in the `enRole.properties` file for the notification delivery method.

   true

   The default is true. Send the recipient an email with the password.

   false

   Send the recipient a link to a website. The recipient must have an email address and a shared secret specified in the personal profile. On the website, the user is asked for the shared secret. If the value that the user enters for the shared secret is correct, the user is taken to a Web site that shows the new password.

   If the user does not specify a shared secret in their personal profile, the user must leave the field on the website blank when it asks for the shared secret.

   If the request is for a manual service, the process sends a work order to the service owner. You can modify the manual work order, including the manual email notification activity.

Creating password strength rules

You can create a password policy that defines the rules to which passwords must conform. For example, password strength rules might specify that the minimum number of characters of a password must be five. The rules might specify that the maximum number of characters must be 10.

Before you begin

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

By default, the Service owner persona can view this task and create password policies for the services the owner persona owns. Furthermore, users who can view this task and have appropriate ACI permissions can create password strength rules.

About this task

To set the password strength rule for a service, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.
2. Create a password policy or change an existing one. Ensure that you selected a service on the Targets tab to which you apply the password policy.
3. Using the Rules tab for the password policy that you select, specify the rules that determine whether a password entry is valid.

Enabling forgotten password authentication

When a user forgets the IBM Security Identity Manager password and must reset it, the user must verify credentials with the system.

Before you begin

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

About this task

An administrator typically defines the forgotten password challenges for a user to attempt a forgotten password recovery.

Note: This task is effective only if a WebSphere account repository is specified. This field is on the ITIM Service **Manage Services** > **Change a Service** > **Service Information** page. This repository can be ITIM Service or a service managed by the Security Identity Manager server. If no registry is specified, the forgotten password option is not available on the Login page.

Respond to a set of forgotten password challenges with answers that you previously specified. Responses are not case-sensitive by default, because the *enrole.challengeresponse.responseConvertCase* property from the `enRole.properties` file has a default value that is lower. The answers are stored in lowercase in the directory server. An answer that you entered is converted to lowercase while it is compared with the stored answers. If you want answers to be case-sensitive, change the value for *enrole.challengeresponse.responseConvertCase* from `lower` to `none`.

Note: The requirement that a user must answer the challenge questions is configurable. By default, the user can bypass the challenge questions. You can force the user to respond to the challenge questions by modifying the property *ui.challengeResponse.bypassChallengeResponse* in the `ui.properties` file. To force user response, set the value to `false`. For more information, see the `ui.properties` topic in the **Reference** > **Supplemental property files** section.

Configuring administrator-defined forgotten password questions

You can enable forgotten password settings for challenge response authentication.

Before you begin

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

About this task

An administrator sets up password challenges for users, which the users must complete before recovering their lost password. When a user answers the administrator-defined challenges successfully, different options are available to receive the new password. To set the right configuration of password recovery, you must complete these steps.

Procedure

1. From the navigation tree, select **Set System Security** > **Configure Forgotten Password Settings**.
2. On the Configure Forgotten Password Settings page, complete these steps:
   a. Select the **Enable forgotten password authentication** check box.
   b. Under the **Login Behavior** field, select one of the following login options.
      - Click **Reset and e-mail password** if you want the system to reset the password and email the password to the user after they successfully answer the challenge response questions. Optionally type in a message the user receives if the user fails to enter the correct answers. Type an email address to which the message is sent.
      - Click **Email user a link to change password** if you want the system to send an email to the user with the link to change the password. A user can click the link in an email that prompts the user to change the password. This option is set to default in the Identity Service Center when you access it through the virtual appliance.

        Note:
        – The **Email user a link to change password** configuration option is effective only when a user initiates the forgot password flow through the Identity Service Center.
        – If a user initiates the forgot password flow through the Self-service user interface, the system prompts the user to change the password and then logs in the user to the system.
   c. Click **OK** to save your changes.
3. On the Success page, click **Close**.

Excluding specific passwords

You can configure the system to prevent users from using specific words as passwords for their accounts.

Before you begin

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

About this task

Specified words are stored in a password dictionary in the LDAP Directory Server. This password dictionary contains a list of words that cannot be used as passwords.

This dictionary can be modified through an LDAP browser by creating `erDictionaryItem` entries under the `erDictionaryName=password` entry. Alternatively, you can import an LDIF file with the entries listed into the Directory Server.

The following is an example of an LDIF file with various words to exclude as passwords listed:

```
dn: erword=apple, erdictionaryname=password, ou=itim, dc=com
objectClass: top
objectClass: erdictionaryitem
erWord: apple

dn: erword=orange, erdictionaryname=password, ou=itim, dc=com
objectClass: top
objectClass: erdictionaryitem
erWord: orange
```

The only value that must be modified is the `erword` value. The `erword` value specifies the word that is *not* allowed to be used as a password.

After the password dictionary is populated with the wanted words, the password policies must be modified to use the dictionary. After importing the LDIF file, select the **Do not allow in dictionary** check box on the Rules page of password policies.

Passwords for system users

After you install IBM Security Identity Manager, three system users are defined. These system users enable IBM Security Identity Manager to communicate with the database and the directory server.

By default, the following systems users are defined:

itimuser
: This user is the IBM Security Identity Manager system user. The system user is created manually before the IBM Security Identity Manager installation program was run.

db2admin or db2inst1
: These users are the DB2 system users that are created by the DB2 installation program. If you installed DB2 on a Windows system, the user name is `db2admin`. If you installed DB2 on a Linux system, the user name is `db2inst1`.

ldapdb2
: This user is the LDAP system user.

Initially, the `db2admin` or `db2inst1` user is created by the DB2 installation process with a password that is set to never expire. However, the password for the `ldapdb2` user and `itimuser` users can expire, based on the password policy of your system. If the passwords for these users expire, or are changed, you must reconfigure IBM Security Identity Manager and its associated middleware to use the new password values.

Changing the itimuser user password

You might need to configure IBM Security Identity Manager to use a new password for the `itimuser` user.

Before you begin

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

You must be a system administrator on the IBM Security Identity Manager Server to have access to this task.

About this task

To change the password of the `itimuser` user on the system, complete these steps:

Procedure

1. From the *ISIM_HOME*`/bin` directory, run the `runConfig` tool.
2. From the System Configuration page in the `runConfig` tool, select the **Database** tab.
3. On the Database page, in the **User Password** field, type the new password, and then click **OK**.

Changing the db2admin user password for Windows

When you change the system user password for `db2admin` in Windows, you must also change the password for any service instances that use `db2admin` as a service account. You must change the password for both the DB2 Universal Database™ service instance and the DB2Admin service instance.

Before you begin

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

You must be a system administrator on the IBM Security Identity Manager Server to have access to this task.

About this task

To change the password for the `db2admin` user on the Windows system, complete these steps:

Procedure

1. Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
2. From the Services page, double-click the DB2 Universal Database instance that IBM Security Identity Manager uses.
3. From the Properties page, click the **Log On** tab.
4. On the Log On page, in the **Password** field and the **Confirm password** field, type the new password, and then click **OK**.

What to do next

To change the password for the DB2Admin service instance, repeat these steps, selecting the DB2Admin service. For example, select **DB2 - DB2Admin**.

Changing the ldapdb2 user password

You might need to configure IBM Security Identity Manager to use a new password for the `ldapdb2` user.

Before you begin

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

You must be a system administrator on the IBM Security Identity Manager Server to have access to this task.

About this task

To change the password for the LDAP database user, complete these steps:

Procedure

1. Navigate to the *drive*`:\idsslapd-ldapb2\etc` directory.
2. Edit the `ibmslapd.conf` file with a text editor.
3. In the `ibmslapd.conf` file, locate `ibm-slapdDbInstance: ldapbdb2`.
4. Change the password for the `ibm-slapdDbUserPW` property. The password currently in the file is encrypted. Replace the old password by typing the new password in clear text, and save the change.

Chapter 5. Organization administration

If you are granted the appropriate authority, you can add, delete, and modify elements in the organization tree. You cannot delete an element that has dependent units in it.

The following elements are in the organization tree:

Organization
Identifies the top of an organizational hierarchy, which might contain subsidiary entities such as organization units, business partner organization units, and locations. The organization is the parent node at the top of the node tree.

Organization Unit
Identifies a subsidiary part of an organization, such as a division or department. An organization unit can be subordinate to any other container, such as organization, organization unit, location, and business partner organization.

Business Partner Organization Unit
Identifies a business partner organization, which is typically a company outside your organization that has an affiliation, such as a supplier, customer, or contractor.

Location
Identifies a container that is different geographically, but contained within an organization entity.

Admin Domain
Identifies a subsidiary part of an organization as a separate entity with its own policies, services, and access control items, including an administrator whose actions and views are restricted to that domain.

Administrator domains

An *administrator domain* (admin domain) identifies a subsidiary part of an organization as a separate entity. The entity has its own policies, services, and access control items. The entity also has an administrator whose actions and views are restricted to that domain.

Domain administrators can do only the administrative tasks on their domains. They cannot do system configuration tasks, which are configuration settings that affect the entire system.

An admin domain is considered a type of organization node. To add, change or delete admin domains, complete the steps for adding, changing, or deleting a node in an organization tree.

You can specify an Security Identity Manager user as the administrator of an admin domain. Enter the Security Identity Manager user in the administrator field. The assignment is confirmed. Then, the Security Identity Manager user is granted the appropriate privileges (access control items, or ACIs) to do administration tasks in that domain.

Any Security Identity Manager user who can add, modify, or delete an admin domain can also specify the administrator for the admin domain. This user is either an Security Identity Manager administrator or an Security Identity Manager user. The user has rights to add, modify, or delete an admin domain through ACIs.

Note: Before Security Identity Manager version 5.0, users were not automatically granted rights as the administrator of an admin domain. Instead, ACIs were required to be added manually. With Security Identity Manager version 5.0 and later, the default ACIs automatically grant the domain administrator the rights for administering the admin domain. The domain administrator is a built-in ACI principal.

Making a user a domain administrator

As an administrator, you can make a user the administrator for a domain.

About this task

You can specify an IBM Security Identity Manager user as the administrator of an `administrator` domain. The IBM Security Identity Manager user is granted the appropriate privileges (access control items, or ACIs) to do administration tasks in that domain.

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the **Organization** node, and then click **Create Admin Domain**. The Admin Domain Details page is displayed.
3. Type the administrator domain name and, optionally, a description.
4. Click **Search** to locate a user.
5. On the Select People page, select the check box for the user or users that you want to make domain administrators for the domain, and click **OK**.
6. Click **OK** on the Admin Domain Details page.

Creating a node in an organization tree

As an administrator, or if you have access control item to organizations, you can create a node in an organization tree.

Before you begin

Determine a model that meets organization needs for service management and user management.

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

To create a node in the tree structure, complete these steps:

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the node, and then click **Create**. Nodes that you can select depend on the position of the specific type of business unit. For example, click **Create Location** to create a location business unit.

3. Complete the fields for the node that you create and click **OK**.
4. Click **Close**.

What to do next

Add any additional nodes that your business model requires for service management or user management.

Changing a node in an organization tree

As an administrator, or if you have access control item to organizations, you can change a node in an organization tree.

Before you begin

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

About this task

Nodes that you can select depend on the position or hyperlink of the node that you select within the structure.

To change a node in an organization tree, complete these steps:

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the node, and then click **Change**.
3. On the Details page for the node, change the necessary fields and then click **OK**.
4. Click **Close**.

Deleting a node in an organization tree

As an administrator, or if you have access control item to organizations, you can delete a node in an organization tree.

Before you begin

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

Remove or migrate any subordinate object that exists in the organization tree, below a node that you intend to delete.

About this task

You cannot delete a higher-level node that contains dependent objects, such as organizational units or locations, or users.

To delete a node in an organization tree, complete these steps:

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the node, and then click **Delete**. Nodes that you can select depend on the position that you select within the structure.
3. On the Confirmation page, ensure that the object is your intended target for deletion, and then click **Delete**.
4. Click **Close**.

Chapter 6. Security administration

After planning system security for IBM Security Identity Manager, you must take additional steps to implement specific groups, views, and access control items.

View management

IBM Security Identity Manager provides default views of the tasks that are available for each default group.

A *view* is a set of tasks that a particular type of user can do in the user interface. If you give a user or group a view, you do not give permissions to the user or group to do the functions within that task. You must also define access control items to give the user or group the necessary permissions for the task.

Creating a view

As an administrator, you can create a view of tasks that IBM Security Identity Manager provides. For example, you might restrict the set of tasks that group members have.

Before you begin

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

Determine the subset of tasks that group members might see. Determine whether an access control item might control the tasks that the view makes visible.

- View All Requests is only intended for users that have full, unrestricted access to the audit trail. There is no ACI checking in this view. Use caution when exposing this task in a user's view.
- View All Requests by Service is intended for service and application owners that need in order to view the audit trail related to services they administer. ACIs are applied only when initially searching for a service. ACIs are not applied to any of the request data shown as a result of selecting a service.
- View All Requests by User is intended for the help desk administrators and managers that need in order to view the audit trail related to specific users. ACIs are applied only when initially searching for a user. ACIs are not applied to any of the request data shown as a result of selecting a user.

About this task

You can use the Define Views page to create additional views.

To create a view, take these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Views** > **Define Views**.
2. On the Define Views page, in the **Views** table, click **Create**.

3. In the General tab, type the name and a description of the view. Click **Apply** to save your changes and continue.
4. Select the Configure View tab and, in the tree of tasks, select the tasks that the view provides. Click **OK** to save the changes.
5. On the Success page, click **Close**.

What to do next

You might create a group that has the view that you created.

Changing a view

As an administrator, you can change a view of tasks that IBM Security Identity Manager provides. For example, you might restrict or expand the set of tasks that group members have.

Before you begin

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

Before you begin, determine the subset of tasks that group members see. Determine whether changing an access control item is also needed.

About this task

You can use the Define Views notebook to change existing views.

To change a view, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Views** > **Define Views**.
2. On the Define Views page, in the **Name** field, type information about the view and click **Search**.
3. In the **Views** table, select a view and click **Change**.
4. In the General tab, change the name or description of the view. Click **Apply** to save your changes and continue. Click **OK** to save the changes.
5. In the Configure View tab, in the tree of tasks, select the tasks that the view provides. Click **OK** to save the changes.
6. On the Success page, click **Close**.

What to do next

You might change any associated access control item for the group that has the view that you changed.

Deleting a view

As an administrator, you can delete a view of tasks that IBM Security Identity Manager provides. For example, you might delete a view after creating an alternative view of tasks that group members can use.

Before you begin

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

Ensure that group members have access to an alternative view of tasks.

About this task

You can use the Define Views page to delete existing views.

To delete a view, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Views** > **Define Views**.
2. On the Define Views page, in the **Name** field, type information about the view and click **Search**.
3. In the **Views** table, select a view and click **Delete**.
4. On the Confirm page, ensure that the view is the one you want to delete, and then click **Delete**.
5. On the Success page, click **Close**.

Defining a custom task

As an administrator, you might want to create a custom task for your business or organization. You must define these custom tasks before you can assign them to a view.

About this task

A custom task represents an external web application that provides services beyond what is supplied by IBM Security Identity Manager. It is defined by a unique identifier, a URL, and optional parameters. The task can be associated with Security Identity Manager views such as Auditor, or Supervisor, and others. Only users that are associated with those views have access to the custom task. Custom tasks are defined in the administrative console, and are available in the Identity Service Center if the user is authorized to access the task.

You can select the **Start task in new window** check box to enable the user to view the custom task in a new browser window. By default, this check box is not selected. If you create a custom task without selecting this check box, when the user starts the task in the Identity Service Center, it is started in the inline frame, or iframe, of the browser window that contains the Identity Service Center. However, if you select the check box, when the user starts the task, it is started in a new browser window or tab, depending on the configuration of the browser.

If you create a custom task that specifies a URL corresponding to the Security Identity Manager administrative console, you must select this check box.

Note:

1. If the web application cannot run custom tasks in a browser *iframe*, that is, inline frame, you must select the **Start task in new window** check box.

2. You can disable headers on some applications for better integration. For example, you might want to create a custom task in the Identity Service Center for the Self Service user interface. To turn off headers so that it integrates better with the Identity Service Center, see Customizing website layout.

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Views**.
2. On the Define Views page, click **Manage Custom Tasks** in the **Views** table.
3. In the **Manage Custom Tasks** table, click **Create**.
4. On the Create Custom Task page, type the task identifier suffix for your task. The suffix cannot contain spaces, quotation marks, hash tags, or equal signs. The combination of the identifier prefix and the identifier suffix is the name that identifies your custom task.

   You can define a label for the custom task by editing the `ISIM_HOME/data/CustomLabels.properties` file. The name of the property is `CUSTOM_<Identifier suffix>` (all in capital letters). The value must be what you want to display in the Identity Service Center. For example, if the identifier suffix is `consoleui`, then the property to add to `CustomLabels.properties` can be `CUSTOM_CONSOLEUI = Identity Manager Console UI`.
5. Optional: Type information that describes the custom task in the **Description** field. To enable the translation of the description, add a prefix `$` to the description string and provide a translation for that property in `ISIM_HOME/data/CustomLabels.properties`, where `ISIM_HOME` is the IBM Security Identity Manager installation directory.

   If you want to display `Custom task` as the description of the task in the Identity Service Center, you must enter `$customTask` in the **Description** field. You must also add an entry in `CustomLabels.properties`: `customTask = Custom task`.

   If you want to translate the description in another language, you must edit the `CustomLabels_xx.properties` file, where xx is the locale. For example, `CustomLabels_fr.properties` might have an entry `customTask = Tâche Personnalisée`.
6. Type the URL that links to your custom task.
7. Optional: Type the URL that links to the image you want to display on the task card.
8. Optional: Specify a menu category for the header. You can also select from the two predefined menu categories:

   manageAccess

   requestStatusTodo
9. Optional: Select the **Show on home page** check box to display the task card on the home page.
10. Optional: Select the **Start task in new window** check box to display the custom task in a new browser window when the user starts the task in the Identity Service Center. If the custom task URL corresponds to the Security Identity Manager administrative console, you must select this check box.
11. Optional: Create custom task parameters. Repeat these steps for each custom parameter you want to create.
    a. In the **Task Parameters** table, click **Create**.
    b. Specify a parameter name.
    c. Specify a parameter value

d. Click **OK**.

12. When you are finished, click **OK**. The Success page is displayed.
13. Select an action or click **Close** to return to the Define Views page.

What to do next

You can now assign the custom task to a view.

Changing a custom task

As an administrator, you can change the task parameters that you specified for a customized task.

About this task

After a task is created, you cannot change the identifier prefix, the identifier suffix, or the console.

Selecting the **Start task in new window** check box enables the user to view the custom task in a new browser window. By default, this check box is not selected. If you change a custom task without selecting this check box, when the user starts the task in the Identity Service Center, it is started in the inline frame, or *iframe*, of the browser window that contains the Identity Service Center. However, if you select the check box, when the user starts the task, it is started in a new browser window or tab, depending on the configuration of the browser.

If you change a custom task that specifies a URL corresponding to the Security Identity Manager administrative console, you must select this check box.

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Views**.
2. On the Define Views page, click **Manage Custom Tasks** in the **Views** table.
3. In the **Manage Custom Tasks** table, select a task and click **Change**.
4. Optional: Under Task information, modify the parameters that you want to change.
5. In the Identifier suffix field, if needed, you can define a label for the custom task by editing the `ISIM_HOME/data/CustomLabels.properties` file. The name of the property is `CUSTOM_<Identifier suffix>` (all in capital letters). The value must be what you want to display in the Identity Service Center. For example, if the identifier suffix is `consoleui`, then the property to add to `CustomLabels.properties` can be `CUSTOM_CONSOLEUI = Identity Manager Console UI`
6. Optional: In the **Description** field, to enable the translation of the description, add a prefix `$` to the description string and provide a translation for that property in `ISIM_HOME/data/CustomLabels.properties`, where `ISIM_HOME` is the IBM Security Identity Manager installation directory.

   If you want to display `Custom task` as the description of the task in the Identity Service Center, you must enter `$customTask` in the **Description** field. You must also add an entry in `CustomLabels.properties`: `customTask = Custom task`.

   If you want to translate the description in another language, you must edit the `CustomLabels_xx.properties` file, where xx is the locale. For example, `CustomLabels_fr.properties` might have an entry `customTask = Tâche Personnalisée`.

7. Optional: Create or change custom task parameters.
   a. In the **Task Parameters** table, click **Create** or select a parameter and click **Change**.
   b. Specify a parameter name.
   c. Specify a parameter value
   d. Click **OK**.
8. Optional: Delete custom task parameters.
   a. In the **Task Parameters** table, select one or more parameters and click **Delete**.
   b. On the Confirm page, ensure that the parameters are the ones you want to delete, and then click **Delete**.

   Note: The parameter changes are not saved until you click **OK** to save the updates to the custom task.
9. When you are finished, click **OK**. The Success page is displayed.
10. Select an action or click **Close** to return to the Define Views page.

What to do next

Log in to the Identity Service Center user interface and verify that your changes are applied.

Deleting a custom task

As an administrator, you can delete fromIBM Security Identity Manager custom tasks that you created. For example, you might delete a custom task you no longer need it or after you create an alternative custom task that group members can use.

Before you begin

If a custom task is used in any view, you cannot delete it. Ensure that the task is removed from of all views.

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Views**.
2. On the Define Views page, click **Manage Custom Tasks** in the **Views** table.
3. In the **Manage Custom Tasks** table, select one or more tasks and click **Delete**.
4. On the Confirm page, ensure that the custom tasks are the ones that you want to delete, and then click **Delete**. The Success page is displayed.
5. Select an action or click **Close** to return to the Define Views page.

What to do next

Navigate back to the **Manage Custom Tasks** table to verify that the task no longer are displayed in the table.

Access control item management

An *access control item (ACI)* is data that identifies the permissions that users have for a specific type of resource. The system administrator has access to all functions in the system and is not governed by access control items.

As system administrator, you create an access control item to specify a set of operations and permissions. Then, you can identify which groups use the access control item.

You can create, change, or delete an access control item. A group might be designated as the owner of the access control item. Members of the group can also do these operations. Members can set up access control items within any branch or subtree branch in which the owned access control item is specified.

Beginning with IBM Security Identity Manager 6.0.0.3, a **Global operation** category is available when you create an access control item. Users that are assigned to this access control item are granted permission to call the custom operation.

Access control items can apply to:

- Entity types such as:
  - All account classes (*erAccountItem*). It controls access to any account.
  - A specific account class (for example, *erPosixLinuxAccount*). It controls access to specific accounts of this class.
  - A user (for example, *erExpressPerson*, which is all users). The access control item controls access to personal profiles.
- Operations that users might perform on entity types or global operations. Custom operations are included with IBM Security Identity Manager 6.0.0.3 and later.
- Permissions for operations on attributes of an entity type, such as an email address.
- A set of users. This set can include access privileges of a *principal*. A principal is a predefined relationship that can be granted privileges. For example, the role of a manager might require access to the contact information for immediate subordinates. You can assign an access control item that grants such access to all users with a manager relationship.

IBM Security Identity Manager provides default access control items that define permissions to the user and to members in other groups. For example, a default access control item for accounts grants permission to all users to search for and modify a password on their accounts.

Default access control items

The following tables list the default access control items (ACIs) for IBM Security Identity Manager.

Table 4. Default access control items

Protection category	Name	Type	Principal
Account	Default ACI for Account: Grant All to Help Desk Group for Non-Admin Accounts	erAccountItem	Help Desk Group
Account	Default ACI for Account: Grant All to Supervisor/Domain Admin/Sponsor/ Service Owner/Access Owner	erAccountItem	Supervisor Domain Admin Sponsor/Service Owner Access Owner

Table 4. Default access control items (continued)

Protection category	Name	Type	Principal
Account	Default ACI for Account: Grant Search, Add, Change Password, and All groupMember Operations to Self	erAccountItem	Self
Account	Default ACI for Account: Grant Search to Auditor Group	erAccountItem	Auditor Group
Account	Default ACI for Account: Grant Connect to Domain Admin and Account Owner	erAccountItem	Domain Admin Account Owner
Account Default Template	Default ACI for Account Defaults: Grant Add/Modify/Search to Service Owner	erAccountTemplate	Service Owner
Admin Domain	Default ACI for AdminDomain: Grant All to Domain Admin	SecurityDomain	Domain Admin
Admin Domain	Default ACI for Admin Domain: Grant Search to Service Owner Group/Auditor/Supervisor/Help Desk	SecurityDomain	Service Owner Group Auditor Group Supervisor Help Desk Group
Business Partner Organization	Default ACI for BP Org: Grant All to Supervisor/Domain Admin/Sponsor	erBPOrg	Supervisor Domain Admin Sponsor
Business Partner Organization	Default ACI for BP Org: Grant Search to Help Desk/Auditor/Service Owner Groups	erBPOrg	Help Desk Group Auditor Group Service Owner Group
Business Partner Person	Default ACI for BPPerson: Grant All to Supervisor/Domain Admin/Sponsor/ Help Desk Group	organizationalPerson	Supervisor/Manager Domain Admin Sponsor Help Desk Group
Business Partner Person	Default ACI for BPPerson: Grant Search and Change Password to Self	organizationalPerson	Self
Business Partner Person	Default ACI for BPPerson: Grant Search to Service Owner and Auditor Group	organizationalPerson	Auditor Group
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant All to Supervisor/Domain Admin/Sponsor	Dynamic role	Supervisor Domain Admin Sponsor
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant Search to Auditor Group	Dynamic role	Auditor Group
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant Search to Everyone	Dynamic role	Everyone
Identity Manager User	Default ACI for ITIM User: Grant Add to Service Owner Group	Identity Manager User	Service Owner Group

Table 4. Default access control items (continued)

Protection category	Name	Type	Principal
Identity Manager User	Default ACI for ITIM User: Grant All to Help Desk Group for Non-Admin Accounts	Identity Manager User	Help Desk Group
Identity Manager User	Default ACI for ITIM User: Grant All to Service Owner	Identity Manager User	Service Owner
Identity Manager User	Default ACI for ITIM User: Grant Delegate to Service Owner/Manager/ Help Desk Groups	Identity Manager User	Service Owner Group Manager Group Help Desk Group
Identity Manager User	Default ACI for ITIM User: Grant Search to Self	Identity Manager User	Self
Identity Policy	Default ACI for Identity Policy: Grant All to Domain Admin/Service Owner Group	erIdentityPolicy	Domain Admin Service Owner Group
ITIM Group	Default ACI for ITIM Group: Grant All to Supervisor/Domain Admin/Sponsor	erSystemRole	Supervisor Domain Admin Sponsor
ITIM Group	Default ACI for ITIM Group: Grant Search to Help Desk Group for Non-Admin Group	erSystemRole	Help Desk Group
ITIM Group	Default ACI for ITIM Group: Grant Search to Service Owner Group	erSystemRole	Service Owner Group
Location	Default ACI for Location: Grant All to Supervisor/Domain Admin/Sponsor	Location	Supervisor Domain Admin Sponsor
Location	Default ACI for Location: Grant Search to Help Desk/Auditor/Service Owner Groups	Location	Help Desk Group Auditor Group Service Owner Group
Organizational Unit	Default ACI for Org Unit: Grant All to Supervisor/Domain Admin/Sponsor	Organizational Unit	Supervisor Domain Admin Sponsor
Organizational Unit	Default ACI for Org Unit: Grant Search to Help Desk/Auditor/Service Owner Groups	Organizational Unit	Help Desk Group Auditor Group Service Owner Group
Password Policy	Default ACI for Password Policy: Grant All to Domain Admin/Service Owner Group	erPasswordPolicy	Domain Admin Service Owner Group
Person	Default ACI for Person: Grant All to Supervisor/Domain Admin/Sponsor/ Help Desk Group	inetOrgPerson	Supervisor/Manager Domain Admin Sponsor Help Desk Group

Table 4. Default access control items (continued)

Protection category	Name	Type	Principal
Person	Default ACI for Person: Grant Change Password to Service Owner Group	inetOrgPerson	Service Owner Group
Person	Default ACI for Person: Grant Search/Change Password/View and Change Role to Self	inetOrgPerson	Self
Person	Default ACI for Person: Grant Search to Service Owner and Auditor Group	inetOrgPerson	Auditor Group
Person	Default ACI for Person: Grant Search and role assignment to Privileged Administrator Group	erPersonItem	Privileged Administrator Group
Provisioning Policy	Default ACI for Provisioning Policy: Grant All to Domain Admin/Service Owner Group	erProvisioningPolicy	Domain Admin Service Owner Group
Provisioning Policy	Default ACI for Provisioning Policy: Grant Search to Auditor Group	erProvisioningPolicy	Auditor Group
Recertification Policy	Default ACI for Recertification Policy: Grant All to Service Owner Group	erRecertificationPolicy	Service Owner Group
Recertification Policy	Default ACI for Recertification Policy: Grant Search to Auditor/Manager Groups	erRecertificationPolicy	Auditor Group Manager Group
Report	Default ACI for Access Control Item (ACI) Report: Grant Run to Auditor Group	Access Control Item	Auditor Group
Report	Default ACI for Access Report: Grant Run to Auditor/Service Owner Groups	Access Report	Auditor Group Service Owner Group
Report	Default ACI for Account Report: Grant Run to Auditor Group	Account Report	Auditor Group
Report	Default ACI for Account Requests by an Individual Report: Grant Run to Auditor/Manager Groups	Account Operations Done by an Individual	Auditor Group Manager Group
Report	Default ACI for Account Requests Report: Grant Run to Auditor/Manager Groups	Account Operations	Auditor Group Manager Group
Report	Default ACI for Account on a Service Report: Grant Run to Auditor/Service Owner Groups	Summary of Accounts on Service	Auditor Group Service Owner Group
Report	Default ACI for Approval/Rejection Report: Grant Run to Auditor/Manager Groups	Approvals and Rejections	Auditor Group Manager Group
Report	Default ACI for Audit Events Report: Grant Run to Auditor Group	Audit Events	Auditor Group
Report	Default ACI for Dormant Accounts Report: Grant Run to Auditor/Service Owner Groups	Dormant Accounts	Auditor Group Service Owner Group
Report	Default ACI for Entitlements Granted to an Individual Report: Grant Run to Auditor Group	Entitlements Granted to an Individual	Auditor Group

Table 4. Default access control items (continued)

Protection category	Name	Type	Principal
Report	Default ACI for Individual Access Report: Grant Run to Auditor/Manager/Service Owner Groups	Individual Access	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Noncompliant Accounts Report: Grant Run to Auditor Group	Noncompliant Accounts	Auditor Group
Report	Default ACI for Operation Report: Grant Run to Auditor/Manager Groups	Operation Report	Auditor Group Manager Group
Report	Default ACI for Orphan Accounts Report: Grant Run to Auditor/Service Owner Groups	Orphan Accounts	Auditor Group Service Owner Group
Report	Default ACI for Pending Approvals Report: Grant Run to Auditor/Manager Groups	Pending Approvals	Auditor Group Manager Group
Report	Default ACI for Pending Recertification Report: Grant Run to Auditor/Manager/Service Owner Groups	Accounts/Access Pending Recertification Report	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Policies Governing a Role Report: Grant Run to Auditor Group	Policies Governing a Role	Auditor Group
Report	Default ACI for Policies Report: Grant Run to Auditor Group	Policies	Auditor Group
Report	Default ACI for Recertification History Report: Grant Run to Auditor/Manager/Service Owner Groups	Recertification History Report	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Recertification Policies Report: Grant Run to Auditor/Manager/Service Owner Groups	Recertification Policies Report	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Reconciliation Statistics Report: Grant Run to Auditor/Service Owner Groups	Reconciliation Statistics	Auditor Group Service Owner Group
Report	Default ACI for Rejected Report: Grant Run to Auditor/Manager Groups	Rejected Report	Auditor Group Manager Group
Report	Default ACI for Services Report: Grant Run to Auditor/Service Owner Groups	Services	Auditor Group Service Owner Group
Report	Default ACI for Suspended Accounts Report: Grant Run to Auditor Group	Suspended Accounts	Auditor Group
Report	Default ACI for Suspended User Report: Grant Run to Auditor Group	Suspended Individuals	Auditor Group
Report	Default ACI for User Accounts by Role Report: Grant Run to Auditor Group	Individual Accounts by Role associated with Provisioning Policy	Auditor Group

Table 4. Default access control items (continued)

Protection category	Name	Type	Principal
Report	Default ACI for User Accounts Report: Grant Run to Auditor/Manager Groups	Individual Accounts	Auditor Group Manager Group
Report	Default ACI for User Requests Report: Grant Run to Auditor/Manager Groups	User Report	Auditor Group Manager Group
Separation of Duty Policy	Default ACI for Separation of Duty Policy: Grant All to Owner	erSeparationOfDutyPolicy	Owner
Separation of Duty Policy	Default ACI for Separation of Duty Policy: Grant Search to Auditor Group	erSeparationOfDutyPolicy	Auditor Group
Service	Default ACI for ITIM Service: Grant All to Domain Admin	ITIM	Domain Admin
Service	Default ACI for Service: Grant Add/Reconcile to Service Owner Group	erServiceItem	Service Owner Group
Service	Default ACI for Service: Grant All to Domain Admin	erServiceItem	Domain Admin
Service	Default ACI for Service: Grant Rights to Everyone	erServiceItem	Everyone
Service	Default ACI for Service: Grant Search/Modify/Remove/Reconcile/ recertOverride/ customizeAccountForm/ enforcePolicy/restartService to Owner	erServiceItem	Owner
Service	Default ACI for Service: Grant Search to Access Owner/Supervisor/Auditor Group	erServiceItem	Access Owner Supervisor Auditor Group
Service Group	Default ACI for Service Group: Grant All to Service Owner	erGroupItem	Service Owner
Service Group	Default ACI for Service Group: Grant Search/View Access to Everyone	erGroupItem	Everyone
Service Group	Default ACI for Service Group: Grant Search to Auditor Group/Supervisor	erGroupItem	Auditor Group Supervisor
Service Group	Default ACI for Service Group: Grant All (except for Add operation) to Access Owner	erGroupItem	Access Owner
Service Selection Policy	Default ACI for Service Selection Policy: Grant All to Domain Admin	erHostSelectionPolicy	Domain Admin
Static Organizational Role	Default ACI for Org Role: Grant All to Supervisor/Domain Admin/Sponsor	Organizational Role	Supervisor Domain Admin Sponsor
Static Organizational Role	Default ACI for Org Role: Grant Search/Modify for Everyone	Organizational Role	Everyone
Static Organizational Role	Default ACI for Org Role: Grant Search to Help Desk/Auditor Groups	Organizational Role	Help Desk Group Auditor Group

Table 4. Default access control items (continued)

Protection category	Name	Type	Principal
Workflow Design	Default ACI for Workflow: Grant All to Domain Admin/Service Owner Group	erWorkflowDefinition	Domain Admin Service Owner Group

Creating an access control item

As an administrator, you can create an access control item to specify a set of operations and permissions. Then, you can apply the access control item to the roles and groups that you want to be governed by the access control item.

Before you begin

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

If you create an access control item that applies to a new group, create the group first.

About this task

You can use the Create access control item wizard to create additional access control items.

To create an access control item, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Access Control Items**.
2. On the Manage Access Control Items page, in the **Access Control Items** table, click **Create**.
3. On the Create Access Control Item wizard, on the General page, specify the name of the access control item and a protection category. If you selected **Account** as your protection category, specify an object class. Specify on which business unit the access control item applies, and whether business subunits are also controlled. Specify whether to apply protection to all objects, or to a subset of objects that are selected by a filter statement that you provide. Then, click **Next**.
4. On the Operations page, select one or more operations, and set the permission to Grant, Deny, or None. Then, click **Next**.
5. On the Permissions page, for each **Read** or **Write** field for each attribute, select Grant, Deny, or None. The table might contain multiple pages of attributes. Click the right arrow button to set permissions for other attributes on the other pages. Then, click **Next**.
6. On the Membership page, specify the focus for roles or group membership that this access control item governs.
7. Click **Finish**.
8. On the Success page, click **Close**.

What to do next

You might associate the access control item with a customized group that you previously created.

After you create an access control item or change an existing access control item, run a data synchronization to ensure that other Security Identity Manager processes, such as the reporting engine, use the new or changed access control item.

Changing an access control item

As an administrator, you can change an access control item if necessary.

Before you begin

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

If you change an access control item, investigate in advance which business units and objects are affected by the change.

About this task

You can use the Change access control item notebook to change an existing access control item.

To change an access control item, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Access Control Items**.
2. On the Manage Access Control Items page, type information about the access control item in the **Search information** field, and click **Search**.
3. In the **Access Control Items** table, select an access control item, and then click **Change**.
4. On the General page, you might change the name of the access control item. You can specify applying protection to all objects. Alternatively, you can specify applying protection to a subset of objects that is selected by a filter statement that you provide. Then, click **Apply** to save your changes, or click another tab.
5. On the Operations page, change the permissions for one or more operations. Then, click **Apply** to save your changes, or click another tab.
6. On the Permissions page, change the permissions for one or more attributes. Then, click **Apply** to save your changes, or click another tab.
7. On the Membership page, change who this access control item governs. Then, click **Apply** to save your changes, or click another tab.
8. Click **OK** to save the changes.
9. On the Success page, click **Close**.

What to do next

After you create an access control item or change an existing access control item, run a data synchronization to ensure that other Security Identity Manager

processes, such as the reporting engine, use the new or changed access control item.

Deleting an access control item

As an administrator, you can delete an access control item if necessary. For example, you might create another access control item that replaces the access control item that you intend to delete.

Before you begin

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

Deleting an access control item revokes any authorization granted to the user (member of the access control item) for a particular protection category. Apply your organization's process that changes or transfers the membership of an access control item before deleting the access control item from the system.

About this task

To delete an access control item, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Access Control Items**.
2. On the Manage Access Control Items page, type information about the access control item in the **Search information** field, and click **Search**.
3. In the **Access Control Items** table, select an access control item, and then click **Delete**. Although you can delete a default access control item that IBM Security Identity Manager provides, you might want to first ensure that an alternative access control item exists.
4. On the Confirm page, ensure that the name of the access control item is correct, and then click **Delete**.
5. On the Success page, click **Close**.

Chapter 7. Role administration

Organizational roles are a method of providing users with entitlements to managed resources. Organization roles determine which resources are provisioned for a user or set of users who share similar responsibilities. A role is a job function that identifies the tasks that a person can do and the resources to which the person has access.

If users are assigned to an organizational role, managed resources that are available to that role then become available to the users in that role. The resources must be properly tied to that role.

You can assign a user to one or more roles. Additionally, roles can themselves be members of other roles, in what is termed *child roles* that contribute to role hierarchy.

A role might be a child role of another organizational role, which then becomes a parent role. That child role inherits the permissions of the parent role. A role might be a child role of another organizational role in a provisioning policy. That child role also inherits the permissions of provisioning policy.

Activities are often assigned to roles rather than to individuals. This role-based model lowers the risk that individuals might gain more system access than required by their job function. You can also define policies to prevent users from having multiple roles that result in a conflict of interest.

Role overview

A role, also termed an organizational role, is a modeling concept that serves as a convenience in administering policy.

The descriptive properties of a role, particularly its name, are significant and imply the purpose of the role. For example, a role might be named manager, designer, or auditor. In IBM Security Identity Manager, a role is used to support user and access provisioning.

A role can be used to support different provisioning models:

- Role-based, to automate and to accelerate the process of granting access to resources. A role-based model lowers the risk of individuals who might gain more system access than required by their job or other relationship to a company.

  The operational needs of an enterprise determine the assignment of users to roles. For example, a user might have a role as a help desk assistant or auditor. In a role-based model, users receive a specific set of accounts and access rights based on role membership. When a user is removed from a role, the entire set of accounts and access rights are also removed.

  The role might be a child role of another organizational role, which then becomes a parent role. The child role inherits the permissions of the parent role.
- Request-based provisioning, in which a role represents an access to an IT resource that can be directly searched and requested by a user.

The access entitlements of the role are defined by a provisioning policy. Approval processing can be supported for a role request; the user is assigned to the role after the request is approved. When the user is a member of a role, access rights are granted. Removing a user from that role also removes the entire set of access that the role granted.

If a role is a child role of another organizational role in a provisioning policy, then that child role also inherits the permissions of provisioning policy.

Using the processes provided by Security Identity Manager, a user in a business unit might have a role as illustrated in the simplified diagram in Figure 1:

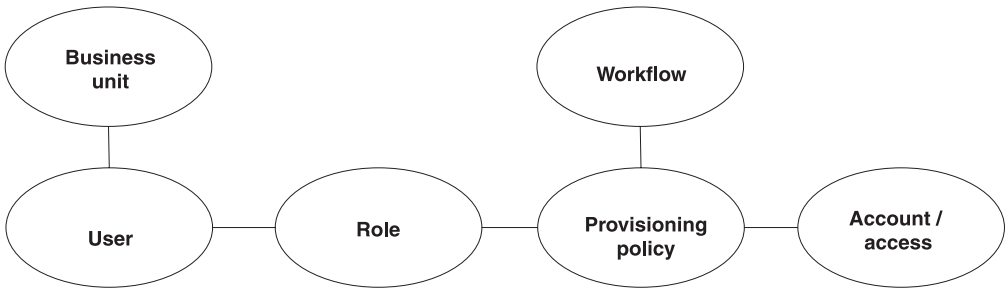


Figure 1. User access to resources

To enable the user to access one or more resources, a provisioning policy can be configured so that the reference role in the policy is granted with the set of entitlements for the resources.

Security Identity Manager also supports two ways to define an organizational role: static role and dynamic role. For a static organizational role, assigning a person to a static role is a manual process. For a dynamic role, role membership is specified as a filter in the role definition that selects role members based on some attribute, such as a business title.

Role hierarchy change enforcement

The people affected by the role hierarchy change operation are evaluated against all applicable policies in the system. Evaluation includes policies that are not related to any of the parent roles. As a result, you might find accounts not related to the role hierarchy change that is being enforced.

For example, you might have a group of new users from an HR feed that did not have workflow enabled. This group of people is entitled to accounts on *Service A* automatically, but the accounts are not created because the HR feed bypassed policy evaluation. A role hierarchy change operation might affect the same group of users so that they are provisioned to *Service B*. Accounts on both *Service A* and *Service B* are created.

Creating roles

You can create roles to allow users to use managed resources, depending on their membership in the role.

Before you begin

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

Determine the range of roles that organization members require to access resources.

About this task

To create a role, complete these steps:

Procedure

1. From the navigation tree, select **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, in the **Roles** table, click **Create**. The Create Role wizard is displayed.
3. On the Role Type page, specify the appropriate values and click **Next**. The pages vary, depending on whether you specify a static or a dynamic role. Complete each page to specify the necessary information for the role.

   Note: On the Access Information page, you can provide owner information and other access information such access type, name, description, search terms, or badges.
4. Click **Finish** when you are done specifying all the expected information.
5. On the Success page, click **Close**.

What to do next

You might associate a provisioning policy with the role that you created.

Modifying roles

You can modify roles that allow users or other roles to use managed resources, depending on their membership in the role.

Before you begin

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

Determine the effects of the change. For example, determine whether changing the scope or the filter definition for a dynamic role correctly limits or expands which users can access resources.

About this task

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.

b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

c. In the **Roles** table, click the icon (▸) next to the role that you want to modify, and then click **Change**. The Change Role wizard is displayed.

3. On the Change Role wizard, edit or modify the existing information on each corresponding page for the role. The pages vary, depending on whether you specify a static or a dynamic role.

   Note: On the Access Information page, you can provide owner information and other access information such access type, name, description, search terms, or badges.

4. Click **OK** when you are done specifying all the expected information on one or all the pages.

Results

A Success page is displayed, indicating that you successfully updated the role.

What to do next

On the Success page, click **Close**.

Values and formats for CSV access data (role)

A role access CSV file can contain multiple values and supported formats.

Consider these points before you work with any CSV files for a role access:

- If you use a custom label for AccessType, specify the key in the CSV file.
- If you use a custom label for badge text, add a $ prefix on the key. For example, $mail.
- Define multiple values for search terms and badges with a semicolon (;) separator.
- Define the AccessType hierarchy with a colon (:) separator.
- Use the badgeText~badgeStyle format for badges.

Define CSV columns for a role access as follows:

Table 5. CSV fields and values. CSV fields and values

Field name	Value
ROLE_DN, ROLE_NAME	Not modifiable.
DEFINE_AS_ACCESS	TRUE or FALSE. If you do not assign any value, then FALSE is assumed.
ACCESS_NAME	Required for services and groups, and contains a maximum length of 240 characters. This field is not available for roles.
ACCESS_TYPE	Required. You must specify an access type that is defined in IBM Security Identity Manager.
ACCESS_DESCRIPTION	Contains a maximum length of 240 characters.
ICON_URL	Provide a valid icon URL value on the access definition.
SEARCH_TERMS	Each search term contains a maximum length of 80 characters. You can have multiple search terms.
ADDITIONAL_INFORMATION	Contains a maximum length of 1024 characters.
BADGES	The maximum length for each badge text is 512 characters. You can have multiple badges. The badge text that is prefixed with a $ sign cannot contain delimiter characters such as ., ;, =, or white space.

A role access CSV file for an export or import operation in the IBM Security Identity Manager administration console contains these columns with sample values and supported formats:

Table 6. Part 1 of 2: Role access CSV file values, formats

ROLE_NAME	DEFINE_AS_ACCESS	ACCESS TYPE	ICON_URL
admin	TRUE	Application:Role:Manager	/itim/ui/custom/ui/images/homepage/RequestAccess.png
AIX Role	TRUE	Mail:Role	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg
Default Role	FALSE	AccessRole	/itim/ui/custom/ui/images/homepage/RequestAccess.png

Table 7. Part 2 of 2: Role access CSV file values, formats

ROLE_NAME	SEARCH_TERMS	ADDITIONAL_INFORMATION	BADGES	SERVICE_DN
admin	Application; Role access	Role that is used by a client user.	$admin~yellow;custom~green	erglobalid=562867050689119980 3,ou=roles,erglobalid=000000
AIX Role	Employee;Role;Role access	Used by the customer to deploy server.	Role~grey	erglobalid=562866975213090286 9,ou=roles,erglobalid=000000
Default Role	Mail;Unique ID	BVT server that is used to run BVT from developer and tester.	$mailrisk~red	erglobalid=562867033703021524 5,ou=roles,erglobalid=000000

Exporting access data for a role

Export the access data for a role in a comma-separated value (CSV) file format by using the IBM Security Identity Manager Console.

Before you begin

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

Before you export a role, you must have ACI privileges for `Search Operations`, and read permissions for the `Access Options` attribute, on the role that you want to view. If the necessary privileges do not exist, then the role is not exported.

The **Export Access Data** button is not active until you select some role accesses to activate it. Only the role access that you selected is exported as access data.

About this task

Export the selected role access data in a CSV file format for your requirements.

Procedure

1. From the navigation tree, select **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, in the **Roles** table, click **Export Access Data**. The Export access data page is displayed. After you submit the export request, a process status indicates the advancement of the export operation.
3. Optional: Click **Cancel** to discontinue the export operation.
4. Click **Download Exported File** to download the CSV file on your local system by using your web browser settings. The exported CSV file contains all the role access data.

   Note: Click **Download Export Log File** to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Results

The exported CSV file contains all the access data for a role. Click **Close** to exit from the Export access data page.

What to do next

Import access data for a role, or you can continue to export access data by clicking **Export Access Data** in the Manage Roles page.

Importing access data for a role

Use the IBM Security Identity Manager Console to import the role access data from a comma-separated value (CSV) file.

Before you begin

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

The privileged user that uploads the CSV file must have the appropriate permissions.

Before you import a role, you must have ACI privileges for `Search Operation`, `Modify Operation`, and read permissions for the `Access Options` attribute, on the role that you want to update. If the necessary privileges do not exist, then the role is not imported.

Before you import a CSV file, verify that the CSV-related conventions are met. They are as follows:

- The access type hierarchy is represented in the following format, and each access type be separated by a colon (`:`). For example:
  ```
  AccessType1:AccessType2
  ```
- The badge information is provided in the following format. For example:
  ```
  badgeText~badgeStyle
  ```
- Multiple badges can be assigned to accesses in the following format, and each badge must be separated by a semicolon (`;`). For example:
  ```
  Badge1~red;Badge2~green
  ```
- Multiple search terms and access types can be specified by using the semicolon (`;`) separator.
- The relevant keys must be provided in the CSV file for the customized labels that are related to badges and access types.

About this task

Only the accesses with the **Define as Access** set to `True` are defined as accesses, and the corresponding data is imported.

Procedure

1. From the navigation tree, select **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, in the **Roles** table, click **Import Access Data**. The Import access data page is displayed.

3. Click **Browse** in **File to Upload (.CSV)** to locate and upload a valid CSV file that contains all the access data for a role.
4. Click **Import** to import the CSV file. After you submit the import request, a process status indicates the advancement of the import operation.

   Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

   If any problems occur when you are importing a CSV file, then close the Import access data page to continue working with the IBM Security Identity Manager Console. The problems might be due to one of the following conditions:

   - The access data CSV file does not exist.
   - The CSV file was renamed.
   - The CSV file does not contain appropriate separators or delimiters.
5. Optional: Click **Cancel** to discontinue the import operation.

   Note: Click **Download Import Log File** to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Results

The imported CSV file contains all the access data for a role. Click **Close** to exit from the Import access data page.

What to do next

Export access data for a role, or you can continue to import access data by clicking **Import Access Data** in the Manage Roles page.

Classifying roles

You can assign a classification to a role.

Before you begin

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

About this task

You can classify a role during role creation, or after a role is already created.

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

c. In the **Roles** table, click the icon (▸) next to the role, and then click **Change**. The Role Type page is displayed.

3. On the Role Type page, complete these steps:
   a. Select a role classification, such as **Application role** or **Business role**, from the **Role classification** list, and then click **OK**. By default, no role classification is selected.

Results

A Success page is displayed, indicating that you successfully updated the role.

What to do next

On the Success page, click **Close**.

Specifying owners of a role

You can specify one or more owners of a role. The owners can be users or roles. You can specify owners of a role during role creation, or after a role is already created.

Before you begin

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

About this task

The result of designating people or roles as a role owner include:

- In workflows, role owners can act as participants. In particular, in the approval workflow for assigning roles to users, role owners can act as participants.
- In access control item (ACI) evaluations for management of roles, the role owner can act as a principal. This capability allows more than one person to share this delegated administrative responsibility. A special case of this scenario is when the role is an owner of itself. In that case, the members of the role can also be the administrators. You can set up a structure so that any member of the role can add other members.
- In exporting roles, the relationships to the role owners are also exported. Relationships to users that are role owners are exported, but the users themselves are not exported. On import, the ownership relationships are created only if the users exist in the import.

In any of these scenarios, being a child or member of a child role of a role owner is equivalent to being a child or member of the role itself.

To specify roles and users that have ownership of the role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:

a. Type information about the role in the **Search information** field.
b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

c. In the **Roles** table, click the icon ( ) next to the role, and then click **Change**. The Role Type page is displayed.

3. Click **Access Information**.
4. On the Access Information page, complete these steps:

   a. Click the twisty icon next to **Owners**. The **Role Owners** and **User Owners** tables are displayed.
   b. Click **Add** to add owners to a list of role owners or user owners. You can select role owners, user owners, or a combination of both. The Select Roles or Select Users page is displayed.
   c. On the Select Roles or Select Users page, search for and select the owners to have ownership of the role, and then click **OK**.

Results

The Access Information page is displayed, and the list of owners is updated in the **Role Owners** and **User Owners** tables.

What to do next

You can continue adding or removing owners of the role, or click **OK**.

Displaying a role-based access in the user interface

You can display an access based on a role to users who request access in the Identity Service Center user interface.

Before you begin

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

About this task

You can use the Manage Roles page to display an access in the Self Service or the Identity Service Center user interface.

To display an access in the Self Service or the Identity Service Center user interface, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.

b. In the **Search by** field, specify whether the search is done against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

c. In the **Roles** table, click the icon (▸) next to the role that you want to modify, and then click **Change** to display the Role Type page.

3. Click the **Access Information** tab.
4. On the Access Information page, click **Enable access for this role**.
5. For a static role, click **Show this role as a common access** to show the role as an access that a user can select.
6. On the Access Information page, select an access type, such as **Application** in the **Select access type** tree. You can also specify other access information such as description, search terms, more information, or badges.
7. Click **OK**.

Results

A Success page indicates that you successfully updated the role.

What to do next

On the Success page, click **Close**.

You might change the provisioning policy that is associated with the role that has the access type.

Role assignment attributes

You can define role assignment attributes. The attributes can be associated with a person-role relationship.

Optional role assignment attributes tasks are:

- Defining role assignment attributes when creating or modifying a static role.
- Associating a custom label with each assignment attribute.
- Specifying assignment attribute values when adding user members to the role. For example, a static role named *Clerk* has an assignment attribute defined as `CreditLimit`. When adding user members to this role, you can specify the `CreditLimit` value for each user as part of the role assignment.
- Specifying assignment attribute values to the existing user members of the role.

Notes:

1. Only static roles support assignment attributes.
2. Only the string type and text widget of assignment attributes are supported.

ACI capabilities for role assignment attributes

Both the default and new ACIs supports attribute-level permissions for role assignment attributes like other attributes in the role definition. You can now modify or create ACIs. You can set attribute-level permissions for granting or

denying usage of these role assignment attributes within the role definition. Only authorized users can read or write assignment attributes. Additionally, you can:

- Set ACIs to read or write assignment attribute values when adding a user to the role.
- Set assignment attribute values to the existing user members.

ACI works the same way as it does for other entities. There is not ACI on specific role assignment attributes. The following attributes are available:

- `erRoleAssignmentKey` is on the role that dictates the permission to define role assignment attributes on the role and an attribute.
- `erRoleAssignments` is on the person that dictates the permission to assign values for the assignment attributes.

You cannot define ACI on the assignment attribute that you defined on the role.

JavaScript capabilities for role assignment attributes

You can access these capabilities for role assignment attributes within the JavaScript interface:

- The role assignment attributes of the role schema. For example, you can access a role object inside an entitlement workflow.
- The role assignment attributes and their values for users in role membership. For example, you can access a person object within a JavaScript provisioning policy entitlement.

New JavaScript APIs include:

- Person
  - Person.getAllAssignmentAttributes()
  - Person.getRoleAssignmentData()
  - Person.getRoleAssignmentData(String roleAssignedDN)
  - Person.removeRoleAssignmentData()
  - Person.updateRoleAssignmentData()
  - Person.getRemovedRoles()
  - Person.isInRole()
  - Person.removeRole()
- Role
  - Role.getAssignmentAttributes()
  - Role.getAllAssignmentAttributes()
  - Role.setAssignmentAttributes()
- RoleAssignmentAttribute
  - RoleAssignmentAttribute.getName()
  - RoleAssignmentAttribute.getRoleName()
  - RoleAssignmentAttribute.getRoleDN()
- RoleAssignmentObject
  - RoleAssignmentObject.getAssignedRoleDN()
  - RoleAssignmentObject.getDefinedRoleDN()
  - RoleAssignmentObject.addProperty()
  - RoleAssignmentObject.getChanges()
  - RoleAssignmentObject.getProperty()

- RoleAssignmentObject.getPropertyNames()
- RoleAssignmentObject.removeProperty()
- RoleAssignmentObject.setProperty()

For more information, see the reference pages in the *IBM Security Identity Manager Reference Guide*.

Role assignment attributes and the Self Service or the Identity Service Center user interface

For more information about adding or modifying role assignment attributes for a user profile in the Self Service or the Identity Service Center user interface, see the IBM Security Identity Manager Support Portal website.

Defining assignment attributes when creating a role

When creating a role, you can optionally define assignment attributes to be associated with the role.

Before you begin

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

You can associate a custom label with an assignment attribute by adding an attribute name prefixed with roleAssignmentAttribute in the `customLabels.properties` resource bundle. This operation provides the display label for the assignment attribute. For example, `roleAssignmentAttribute.creditLimit="Credit Limit Value"`. The key for the assignment attribute of the same role must be unique.

Procedure

To define assignment attributes to be associated with a role, complete these steps:

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, click **Create** and proceed through the wizard panels until you reach the Assignment Attributes page. If you selected a role type of `Dynamic`, the Assignment Attributes page is not displayed.
3. In the **Attribute Name** field, specify a name for the assignment attribute you want to add.

   Note: You must not enter a space, semi-colon, or both when specifying an assignment attribute name.
4. Click **Add**.

   The new attribute is displayed in the assignment attributes table. If the attribute has any display label defined in the `customLabels.properties` resource bundle, then the assignment attribute table displays the same label.
5. Click **Next** to continue through the Role Creation wizard.

Results

A Success page is displayed, indicating that you successfully created the role.

Defining assignment attributes for an existing role

When modifying an existing role, you can optionally define assignment attributes to be associated with the role.

Before you begin

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

You can associate a custom label with an assignment attribute by adding an attribute name prefixed with roleAssignmentAttribute in the `customLabels.properties` resource bundle. This operation provides the display label for the assignment attribute. For example, `roleAssignmentAttribute.creditLimit="Credit Limit Value"`. The key for the assignment attribute of the same role must be unique.

Procedure

To define assignment attributes to be associated with a role, complete these steps:

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Roles** table, click the icon (▸) next to the role, and then click **Change**. The Role Type page is displayed.
3. Click **Assignment Attributes**. The Assignment Attributes page is displayed. If you selected a role type of `Dynamic`, the Assignment Attributes page is not displayed.
4. To add an attribute to an existing role, enter a name in the **Attribute Name** field for the assignment attribute you want to add.

   Note: You must not enter a space, semi-colon, or both when specifying an assignment attribute name.
5. Click **Add**.

   The new attribute is displayed in the assignment attributes table. If the attribute has a display label defined in the `customLabels.properties` resource bundle, then the assignment attribute table displays the same label.
6. Optionally, you can remove existing assignment attributes if no values are set with any user member of the role.

Results

A Success page is displayed, indicating that you successfully updated the role.

Setting assignment attribute values to the user members of a role

You can set assignment attribute values to the user members of a static organizational role if you defined assignment attributes in the role definition.

Before you begin

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

Procedure

To set assignment attributes to the user members in a static role, complete these steps:

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Roles** table, click the icon (▸) next to the role to which you want to add members, and then click **Manage User Members**. The Manage User Members and Child Roles page is displayed.
3. On the Manage User Members and Child Roles page, complete these steps:
   a. Type information about the user in the **Search information** field.
   b. In the **Search by** field, select the attribute on which you want to search, and then click **Search**, or click **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. The **Users** table is displayed, listing the users that match the search criteria.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Users** table, select the check box next to one or more user members that you want to set assignment attribute values, and then click **Set Assignment Attributes**. Selecting the check box at the top of this column selects all user members. The Associate Role Assignment Attributes page is displayed.

   Note: The Associate Role Assignment Attributes page is displayed if you defined role assignment attributes when creating the role. These conditions apply:
   - When the role is a child role to one or more parent roles, the role assignment attributes includes the attributes from all of the parent roles.
   - When you select a user member, the existing attribute value is displayed if you assigned values when adding user members.

- The values are not displayed if you have not set any of them in the assignment attributes when adding user members.
- When you select multiple user members, the values for assignment attributes are joined.

4. On the Associate Role Assignment Attributes page, complete these steps:
   a. Enter values for the role assignment attributes.

      In the role assignment attributes table, click the name of the assignment attribute. The Set Assignment Values page is displayed.
   b. Enter a value for the attribute and click **Add**. You can add more than one value. When finished, click **OK.**

      The **Associate Role Assignment Attributes** table is displayed.
   c. When finished adding values to attributes, click **Continue**. A confirmation page is displayed.
5. On the Confirm page, specify the date and time for the user members to be added with the assignment attribute values. Then click **Submit**. Click **Back** to return to the previous page.

Results

A Success page is displayed, indicating that you successfully added the user members to the role membership.

What to do next

View the status of the request, or click **Close**.

Configuring access catalog information for a role

Configure the access catalog information for a role in the Administrator Console so you can use it in the Identity Service Center Request Access.

Before you begin

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

You can also configure the access catalog information for a new role or for an existing role.

About this task

Configure the access information for a role by defining certain accesses with the use of a badge. You can highlight certain accesses with badges by attaching text that contains some formatting such as color and font type.

Procedure

To configure the role access information, complete these steps:

1. From the navigation tree, select **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, in the **Roles** table, click **Create** to display the Create Role wizard. Alternatively, select an existing role and click **Change** to configure its access catalog information.

3. Specify the appropriate values on the Role Type page. The pages vary, depending on whether you specified a static or a dynamic role.
4. Specify the appropriate values on the General Information page.
5. On the Access Information page, complete these steps to configure the access information:
   a. Expand the **Owners** section to specify the roles or users that are the owners of the role.
   b. Select the **Enable access for this role** check box.
   c. Expand the **Select access type** or the **Change access type** tree to select an access type. The tree label depends on whether you want to create or modify a service.
   d. Provide a uniform resource identifier (URI) string in the **Icon URL** field for the access icon.
   e. Specify search strings in the **Search terms** field to return specific search terms. Add or delete the search terms to suit your requirements.
   f. Specify any free form information about the access item in the **Additional information** field.
   g. Expand the **Badges** section to specify the badges that are associated with the role.
      - Specify a badge text in the **Badge text** field.
      - Assign a class from the **Badge class** list for the badge text.

      You can see the preview of your badge specifications in the **Preview** area.
6. Depending on whether you created or modified the role access information, click **OK** or **Finish** when you are done.

Results

The access information is added to the role object and stored in the Security Identity Manager LDAP server.

What to do next

On the Success page, click **Close**.. You can also do the following actions:

- Create or modify another role
- Return to the list of roles that you were working with

Deleting roles

You can delete roles that allow users to use managed resources, depending on their membership in the role.

Before you begin

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

About this task

You cannot delete a role that has user members or child roles. You must remove all of the user members and child roles from the role before you can delete the role.

You cannot delete a static role that has membership in a policy, such as a provisioning or separation of duty policy. You must first remove the static role from the policy.

To delete a role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Roles** table, select the check box next to the role that you want to delete, and then click **Delete**. Selecting the check box at the top of this column selects all roles. A confirmation page is displayed.
3. On the Confirm page, click **Delete**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the role.

What to do next

Continue working with roles, or click **Close**.

Managing users as members of a role

You can view, add, or remove *user members*, which are users that are members of a role.

Before you begin

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

About this task

To manage user members, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Roles** table, click the icon (▸) next to the role, and then click **Manage User Members**. The Manage User Members and Child Roles page is displayed.
4. On the Manage User Members and Child Roles page, complete these steps:
   a. Select **User member**.
   b. Type information about the user in the **Search information** field.
   c. In the **Search by** field, specify the attribute on which you want to search, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.

Results

The **Users** table is displayed, listing the user members that match the search criteria.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

You can add user members to the role or remove user members from the role. You can also set assignment attribute values to user members of a role.

Click **Close** to close the page.

Adding users to membership of a role

You can add a user to the membership of a static organizational role.

Before you begin

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

About this task

To add a user to membership in a static role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

c. In the **Roles** table, click the icon (▸) next to the role to which you want to add members, and then click **Add User Members**. The Add User Members page is displayed.

3. On the Add User Members page, complete these steps:
   a. Type information about the user in the **Search information** field.
   b. In the **Search by** field, select the attribute on which you want to search, and then click **Search**, or click **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. The **Users** table is displayed, listing the users that match the search criteria.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Users** table, select the check box next to one or more users that you want to add to the membership of the role, and then click **OK**. Selecting the check box at the top of this column selects all users. You cannot select a user that is already a member of the role. The Associate Role Assignment Attributes page is displayed.

   Note: The Associate Role Assignment Attributes page is displayed only if you defined role assignment attributes when creating the role.
4. On the Associate Role Assignment Attributes page, complete these steps:
   a. Enter values for the role assignment attributes.
   b. Click **Continue**. A confirmation page is displayed.
5. On the Confirm page, specify the date and time for the user members and role assignment attributes to be added. Then click **Submit**. Click **Back** to return to the previous page.

Results

A Success page is displayed, indicating that you successfully added the user members to the role membership.

What to do next

View the status of the request, or click **Close**.

Removing users from membership of a role

You can remove a user from membership in a static role.

Before you begin

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

About this task

To remove a user from membership in a static role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Roles** table, click the icon (▸) next to the role, and then click **Manage User Members**. The Manage User Members and Child Roles page is displayed.
3. On the Manage User Members and Child Roles page, complete these steps:
   a. Select **User**.
   b. Type information about the user in the **Search information** field.
   c. In the **Search by** field, specify the attribute on which you want to search, and then click **Search**, or click **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. The **Users** table is displayed, listing the users that match the search criteria.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   d. In the **Users** table, select the check box next to the user member that you want to remove from membership in the role, and then click **Remove**. Selecting the check box at the top of this column selects all user members. A confirmation page is displayed.
4. On the Confirm page, specify the date and time for the membership removal to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the user members from the role membership.

What to do next

View the status of the request, view the membership of the role, or click **Close**.

Managing child roles

You can view, add, or remove *child roles*, which are roles that are members of another role. This relationship is a parent-child relationship between an organizational role (a parent role) and its child roles. A child role itself is an organizational role.

Before you begin

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

complete it for you, contact your system administrator.

About this task

When you add child roles to a parent role, ensure that there is not a separation of duty policy violation.

To manage child roles, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Roles** table, click the icon (▸) next to the role, and then click **Manage Child Roles**. The Manage User Members and Child Roles page is displayed.
4. On the Manage User Members and Child Roles page, complete these steps:
   a. Select **Child role**.
   b. Type information about the role in the **Search information** field.
   c. In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**.

Results

The **Child Roles** table is displayed, listing the child roles that match the search criteria.

If the table contains multiple pages, you can:
- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

You can add more child roles to the parent role, or you can remove child roles from the role.

Click **Close** to close the page.

Adding child roles to a parent role

You can add a role (child role) to the membership of an organizational role (parent role). This task defines the roles in a role hierarchy. Circular parent-child relationships are not permitted.

Before you begin

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

About this task

When you add child roles to a parent role, ensure that there is not a separation of duty policy violation.

To add a child role to a parent role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Roles** table, click the icon (▸) next to the role, and then click **Add Child Roles**. The Add Child Roles page is displayed.
3. On the Add Child Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. The **Roles** table is displayed, listing the roles that match the search criteria and that can be children of another role.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Roles** table, select the check box next to one or more roles that you want to add to the membership of the role, and then click **Add**. Selecting the check box at the top of this column selects all roles. You cannot select a role that is already a child role.
   d. Click **OK** to add the selected roles as children of the organizational role, or click **Cancel**.
4. On the Confirm page, specify the date and time for the membership removal to occur, and then click **Submit**, or click **Cancel**.

Results

A Success page is displayed, indicating that you successfully added a child role.

The roles are added as children of the organizational role, and the Manage Roles page is displayed.

What to do next

You can continue working with roles, or click **Close**.

Removing child roles from a parent role

You can remove a child role from a parent role.

Before you begin

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

Determine how removing the role affects the role hierarchy.

About this task

To remove a child role from a parent role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Roles** table, click the icon (▸) next to the role, and then click **Manage Child Roles**. The Manage User Members and Child Roles page is displayed.
4. On the Manage User Members and Child Roles page, complete these steps:
   a. Select **Child role**.
   b. Type information about the role in the **Search information** field.
   c. In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**. The **Roles** table is displayed, listing the roles that match the search criteria and that can be children of another role.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
   d. In the **Roles** table, select the check box next to the child role that you want to remove from the parent role, and then click **Remove**. Selecting the check box at the top of this column selects all child roles. A confirmation page is displayed.
5. On the Confirm page, click **Submit**, or click **Cancel**.

Results

A Success page is displayed, indicating that you successfully removed the child roles from the parent role.

What to do next

You can continue working with roles, or click **Close**.

Creating an access type based on a role

You can create role-based access to resources.

Before you begin

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

About this task

You can use the Manage Access Types page to create an access type.

To create an access type that is based on a role, complete these steps:

Procedure

1. From the navigation tree, select **Configure System** > **Manage Access Types**. The Manage Access Types page is displayed.
2. On the Manage Access Types page, complete these steps:
   a. In the **Access Types** tree, click the icon next to **Role**, and then click **Create Type**. The Create Access Type page is displayed.
   b. On the Create Access Type page, in the **Access type key** field, type a unique name for the access type key that you want to create.
   c. Optional: In the **Description** field, type a description for the access type key that you want to create.
   d. Click **OK**.

Results

The Manage Access Types page is displayed, and the new access type is listed in the **Access Types** tree.

What to do next

You might need to update the `CustomLabels.properties` resource bundle to provide the display label for this new access type.

You might make the new access available to users in the Self Service or the Identity Service Center user interface. To do so, associate the role with the newly created access type.

Chapter 8. Services administration

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

Overview

Services are created from service types, which represent a set of managed resources that share similar attributes. For example, there is a default service type that represents Linux systems. These service types are installed by default when IBM Security Identity Manager is installed. Service types are also installed when you import the service definition files for the adapters for those managed resources.

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

A *service owner* identifies the person who owns and maintains a particular service in IBM Security Identity Manager.

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

Service administration tasks

Service administration tasks are done by using **Manage Services** from the navigation menu. Service administration tasks include the following tasks:

- Creating services and optionally creating provisioning policies for those services
- Changing or deleting services
- Scheduling an account reconciliation or initiating an immediate account reconciliation, including reconciling supporting data only. An immediate account reconciliation reconciles only the data you need for defining provisioning policies and access information for a group.
- Configuring policy enforcement on services, where you define the enforcement action when an account is noncompliant
- Viewing groups and defining access entitlements on groups
- Requesting accounts
- Displaying, changing, removing, suspending, and restoring accounts
- Assigning accounts to users
- Viewing account recertification status
- Displaying, creating, changing, and removing account defaults

Service prerequisite

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

Service types

A *service type* is a category of related services that share schemas. It defines the schema attributes that are common across a set of similar managed resources.

Service types are profiles, or templates, that create services for specific instances of managed resources. For example, you might have several Lotus® Domino® servers that users need access to. Create one service for each Lotus Domino server with the Lotus Domino service type. In previous versions of IBM Security Identity Manager, a service type is called a *service profile*.

Some service types are installed by default when Security Identity Manager is installed. Other service types can be installed when you import the service definition files for adapters for managed resources. A service type definition is provided by the Security Identity Manager adapter for a managed resource. There is a service type for each type of managed resource that Security Identity Manager supports. Some examples are UNIX, Linux, Windows, and IBM Security Access Manager.

A service type is defined in the service definition file of an adapter, which is a Java Archive (JAR) file that contains the profile. The service type for an adapter is created when the adapter profile (JAR file) is imported. For example, a service type is defined in the `WinLocalProfile.jar` file. You can also define a service type with the interface for Security Identity Manager.

Security Identity Manager supports the following types of service providers:

- DAML for Windows Local adapter, Lotus Notes adapter
- IDI (IBM Security Directory Integrator for UNIX and Linux adapters)
- Custom Java class for defining your own implementation of a service provider
- Manual for managing user-defined “manual” activities

Default service types

The following default service types are provided with Security Identity Manager:

Identity feed service types:

DSML
A Directory Services Markup Language (DSML) Identity Feed service imports user data, with no account data, from a human resources database or file. The service feeds the information into the Security Identity Manager directory. The service uses a placement rule to determine where in the organization a user is placed. The service can receive the information in one of two ways: a reconciliation or an event notification. This service is based on the DSML Identity Feed Service Profile.

Note: DSMLv2 is deprecated in Security Identity Manager Version 5.0 in favor of the remote method invocation (RMI)-based IDI adapter framework. The use of DSMLv2 continues to be supported in this release.

AD The AD Identity Feed Service imports user data from Windows Active Directory. The `organizationalPerson` objects are fed into Security Identity Manager and add or update users to Security

Identity Manager. The user profiles that are selected from this service must have an objectclass that is derived from the `organizationalPerson` class.

CSV The CSV Identity Feed Service imports user data from a comma-separated value (CSV) file and adds or updates users to Security Identity Manager. A CSV file contains a set of records that are separated by a carriage return/line feed (CR/LF) pair (`\r\n`). Each record contains a set of fields that are separated by a comma. If the field contains either a comma or a CR/LF, the comma must be escaped with double quotation marks as the delimiter. The first record in the CSV source file defines the attributes that are provided in each of the following records. Attributes must be valid based on the class schema for the selected person profile for this service.

IDI Data Feed
The IDI Data Feed service type uses the Security Directory Integrator to import user data, with no account data, into Security Identity Manager and to manage accounts in the Security Identity Manager data store on external resources. This service is based on the IDI Data Feed Service Profile.

INetOrgPerson
The INetOrgPerson Identity Feed imports user data from the LDAP directory. The inetOrgPerson objects are loaded and add or update users in Security Identity Manager.

Account service types:

Security Directory Integrator-based
This service type can be optionally installed during the installation of Security Identity Manager. All of these services are Security Directory Integrator-based adapters; each is a specific service type. Security Directory Integrator is one type of service provider. There can be multiple service types that are defined for the same type of service provider.

ITIM Service
The ITIM service type is used to create accounts in the Security Identity Manager system and represents the Security Identity Manager itself. This type is a standard service with no configuration parameters. All users that need access to the Security Identity Manager system must be provisioned with an Security Identity Manager account.

Hosted Service
The Hosted Service type is used to create a service that is a proxy to the hosting service that is in the service provider organization.

The hosted service connects to the managed resource target through the hosting service indirectly. The configuration details of the hosting service are invisible and protected from administrators in the secondary organization where the Hosted Service is defined. Administrators can define policies for the hosted service, specifically, without affecting the hosting service.

The primary usage of a Hosted Service is to allow users in business partner organizations to have accounts and access to internal IT resources of an organization. A Hosted Service allows

administrators in the secondary organization to define specific service policies for the user accounts.

Custom Java class
The custom Java class service type defines your own implementation of a service provider.

Manual service type
The Manual service type is used to create a manual service.

Service status

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

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

All Status values for all services.

Alive Services that are functioning with no known issues.

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

Attempting recovery
Services that encountered a problem and for which the server is attempting to process a previously blocked request.

Locked
Services that are locked because a reconciliation process is running.

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

Each status value other than **Alive** provides an icon that links to more detailed information about the state of the service. For example, if the server cannot complete a request due to a network or authentication problem, it marks the service as **Failed**. Until the service recovers from the **Failed** status, provisioning requests cannot be processed. The failing request and any additional account requests are blocked until the problem with the service is corrected. Clicking the **Failed** icon retrieves details about the failure, including the time of the first failure, detailed reason for the failure, and number of blocked requests.

The system periodically checks **Failed** services and attempts to recover the blocked requests. If the problem with the service is corrected, blocked requests can be completed due to this periodic check. The default time interval for the periodic recovery check is 10 minutes.

Restarting of the blocked requests

Retry Blocked Requests provides an option to immediately restart the blocked requests from the Manage Services panel. This action tests a service to see whether the problem is corrected. If the test is successful, it restarts any blocked requests for a failed service. Failures are returned to the user interface so that all configuration problems with the service can be corrected.

When the recovery process is started for a service, the service is placed in **Attempting recovery** status until all blocked requests are restarted. During this time, new requests can proceed normally.

Provisioning requests can also be blocked during reconciliation with the locking feature enabled. In this case, the service status shows **Locked** until the reconciliation completes. At that time, the service status is updated to **Attempting recovery** until any blocked requests are processed. When all blocked requests are restarted, the service returns to the **Alive** status.

Retry Blocked Requests is controlled by a task in the view definitions defined in **Set System Security** > **Manage Views** in the IBM Security Identity Manager administrative console. To restart the blocked requests of a service immediately, select **Manage Services** from the IBM Security Identity Manager administrative console. From the **Services** table and under **Service Name**, click an arrow to the right of the service and select **Retry Blocked Requests**.

Creating services

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

Before you begin

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

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

About this task

If you choose to create a provisioning policy as part of this task, the service is automatically added to the provisioning policy as an entitlement. In addition, a membership of “All” is defined for the provisioning policy. You can later edit the provisioning policy and change the membership after the service is created.

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

To create a service instance, complete these steps:

Procedure

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, click **Create**. The Create a Service wizard is displayed.

3. On the Select the Type of Service page, click **Search** to locate a business unit. The Business Unit page is displayed.
4. On the Business Unit page, complete these steps:
   a. Type information about the business unit in the **Search information** field.
   b. Select a business type from the **Search by** list, and then click **Search**. A list of business units that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**. The Select the Type of Service page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the Select the Type of Service page, select a service type, and then click **Next**.

   If the table contains multiple pages, you can:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the Service Information or General Information page, specify the appropriate values for the service instance. The content of the General Information page depends on the type of service that you are creating. The creation of some services might require more steps.
7. On the Authentication page, configure authentication (either password-based or key-based) for the service, and then click **Next** or **Finish**. The Authentication page is displayed only if you are creating a POSIX service instance.
8. On the Dispatcher Attributes page, specify information about the dispatcher attributes, and then click **Next** or **OK**. The Dispatcher Attributes page is displayed only for IBM Security Directory Integrator based services.
9. Optional: On the Access Information page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable. Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
10. On the Status and Information page, view information about the adapter and managed resource, and then click **Next** or **Finish**. The adapter must be running to obtain the information.
11. On the Configure Policy page, select a provisioning policy option, and then click **Next** or **Finish**. The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the Configure Policy page is not displayed.
12. Optional: On the Reconcile Supporting Data page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**. The Reconcile Supporting Data page is displayed for all services except for identity feed services.

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.

13. Optional: On the Service Information or General Information page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**. If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

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

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table and display the new service instance.

Creating a service that has manual connection mode

If you did not install the adapter for the managed resource, use this task to create an instance of a service. You can use the manual connection mode to manage account requests instead of creating a manual service. After you install the adapter, you can change the connection mode from manual to automatic.

Before you begin

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

To create a service in IBM Security Identity Manager, you must create a service type. Alternatively, use one of the service types that were automatically created when IBM Security Identity Manager Server was installed. To create a service type either:

- Import the adapter profile, or
- Add the new schema classes and attributes for the service to your LDAP directory

You must add the `erconnectionmode` attribute to the customized form for the service type to enable connection mode. See “Enabling connection mode” on page 120.

About this task

This task is for creating a service with manual connection mode before the adapter is installed. After the adapter installation, to create a service with an automatic connection, select **Automatic** and follow the task for creating a service. See “Creating services” on page 115.

If you choose to create a provisioning policy as part of this task, the service is automatically added to the provisioning policy as an entitlement. In addition, a membership of `All` is defined for the provisioning policy. You can later edit the provisioning policy and change the membership after the service is created.

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

To create a service instance that has manual connection mode, complete these steps:

Procedure

1. From the navigation tree, click **Manage Services**. The Select a Service page is opened.
2. On the Select a Service page, click **Create**. The Create a Service wizard is opened.
3. On the Select the Type of Service page, click **Search** to locate a business unit. The Business Unit page is opened.
4. On the Business Unit page, complete these steps:
   a. Type information about the business unit in the **Search information** field.
   b. Select a business type from the **Search by** list, and then click **Search**. A list of business units that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**. The Select the Type of Service page is opened, and the business unit that you specified is shown in the **Business unit** field.
5. On the Select the Type of Service page, select a service type, and then click **Next**.

   If the table contains multiple pages, you can:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the Service Information or General Information page, specify the appropriate values for the service instance. Then, click **Test Connection** to validate that the data in the fields is correct. If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

   Note: The content of the Service Information or General Information page depends on the type of service that you are creating. The creation of some services might require more steps.
7. For the **Connection mode** option, select **Manual**. Selecting **Manual** enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

   Note: This option is available only if the `erconnectionmode` attribute is added to the service form. Connection mode is not supported on the `ITIM Service` or any type of identity feed service, hosted service, or manual service types. For information about adding the `erconnectionmode` attribute, see "Enabling connection mode" on page 120.
8. On the Users and Groups page, specify user and group information for the service.

Note: The Users and Groups page is opened only if you are creating certain service instances.

9. On the Authentication page, configure authentication (either password-based or key-based) for the service, and then click **Next** or **Finish**.

   Note: The Authentication page is displayed only if you are creating a POSIX service instance.

10. Optional: On the Dispatcher Attributes page, specify information about the dispatcher attributes, and then click **Next** or **Finish**.

    Note: The Dispatcher Attributes page is displayed only for Directory Integrator-based services.

11. Optional: On the Access Information page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable. Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
12. Optional: On the Status and Information page, you can view information about the adapter and managed resource, and then click **Next** or **Finish**.
13. On the Participants page, specify the users who are involved in completing the activities for the manual service. Specify the amount of time before the service is escalated. Click **Next**.
14. Optional: On the Messages page, complete these steps, and then click **Next** or **Finish**:
    a. Select the default email message that you want to change, and then click **Change**. The Change Message page is opened.
    b. Modify the **Subject** and **Body** fields, and then click **OK**.
15. On the Configure Policy page, select a provisioning policy option, and then click **Next** or **Finish**. The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only the Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the Configure Policy page is not opened.

16. Optional: On the Reconciliation page, click **Browse** to locate the reconciliation file, and then click **Upload File** to load the new reconciliation file. You can also choose whether to reconcile supporting data only.

    Note: The file type that is supported for the reconciliation file is CSV. For more information, see "Example comma-separated value (CSV) file" on page 139.

Results

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

What to do next

Select another services task, or click **Close**. When the Select a Service page is opened, click **Refresh** to refresh the **Services** table and display the new service instance.

Enabling connection mode

Use connection mode to create a service that can function like either an automated or a manual service.

Before you begin

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

Only individuals who are part of the administrator group can access this feature.

About this task

Before you install the adapter, use connection mode to create a service and to specify the account request route. The account route can be specified as either automatic or manual.

Automatic
Specifies to route account requests to a service provider. This selection is the default setting.

Manual
Specifies to route account requests to a specific user.

Note: Selecting Manual enables the Participants page and a different Reconciliation page in the navigation area of the Create a Service wizard.

The advantage of using connection mode is that you do not need to create and later remove a manual service. After installing the adapter, to change to an automated service, change the connection mode from manual to automated. See "Changing connection mode from manual to automatic" on page 124.

Note: Connection mode is not supported on ITIM service or any type of identity feed service, hosted service, or manual service types. Do not add the erconnectionmode attribute to the forms for those service types.

To enable connection mode, add the erconnectionmode attribute to the service form.

Procedure

1. From the navigation tree, click **Configure System** > **Design Forms**. The form designer applet is displayed.
2. In the left pane, double-click the **Service** folder to display the profiles for the service types. Double-click the service type profile to open the template for that profile. The form template associated with the service type profile is displayed in the middle pane.
3. Select the tab to which you want to add the attribute.
4. In the Attribute List pane, double-click **erconnectionmode**. The attribute is added to the form.
5. Right click **erconnectionmode**. Click **Change To** > **Dropdown Box**.
6. Click **Custom Values**. The Select Editor is displayed to design the drop-down menu.
7. Define the menu.

a. Under **Data Value** type `AUTOMATIC`.
b. Under **Display Value** type `$automatic`.
c. Click the **Add Row** icon.
d. Under **Data Value** type `MANUAL`.
e. Under **Display Value** type `$manual`.
f. Click **OK**.

8. Right click **erconnectionmode**. Click **Move Up Attribute** or **Move Down Attribute** to position the field on the form.
9. Click **Form** > **Save Form Template**, and then click **OK** when a message is displayed, indicating that the form template is saved successfully.
10. Click **Close** to exit Form Designer.

What to do next

Verify that connection mode was added to the service form.

1. Click **Manage Services** > **Create**.
2. Select the service type profile that you modified for connection mode. Click **Next**.
3. Verify that Connection mode is displayed on the form.

Creating manual services

Create a manual service instance when IBM Security Identity Manager does not provide an adapter for the managed resource.

Before you begin

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

Before you can create a manual service in Security Identity Manager, you must create a service type. Add new schema classes and attributes for the manual service to your LDAP directory.

About this task

A manual service is a type of service that requires manual intervention to complete the request. For example, a manual service might be defined for setting up voice mail for a user. A manual service generates a work order activity that defines the manual intervention that is required.

If you choose to create a provisioning policy as part of this task, the service is automatically added to the provisioning policy as an entitlement. In addition, a membership of "All" is defined for the provisioning policy. Also, an ownership type of "Individual" is defined for the provisioning policy. You can later edit the provisioning policy and change the membership and ownership types after the service is created.

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

To create a manual service instance, complete these steps:

Procedure

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, click **Create**. The Create a Service wizard is displayed.
3. On the Select the Type of Service page, click **Search** to locate a business unit. The Business Unit page is displayed.
4. On the Business Unit page, complete these steps:
   a. Type information about the business unit in the **Search information** field.
   b. Select a business type from the **Search by** list, and then click **Search**. A list of business units that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**. The Select the Type of Service page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the Select the Type of Service page, select a manual service type, and then click **Next**.

   If the table contains multiple pages, you can:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On the General Information page, specify the appropriate values for the manual service instance, and then click **Next**. The content of the General Information page depends on the type of service that you are creating. The creation of some services might require additional steps.
7. On the Participants page, specify the users who are involved in completing the activities for the manual service. Specify the amount of time before the service is escalated. Click **Next**.
8. Optional: On the Messages page, complete these steps, and then click **Reconciliation**:
   a. Select the default email message that you want to change, and then click **Change**. The Change Message page is displayed.
   b. Modify the **Subject** and **Body** fields, and then click **OK**.
9. Optional: On the Access Information page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable. Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
10. On the Configure Policy page, select a provisioning policy option, and then click **Next** or **Finish**. The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.
11. Optional: On the Reconciliation page, click **Browse** to locate the reconciliation file, and then click **Upload File** to load the new reconciliation file. You can also choose whether to reconcile supporting data only.

Note: The file type that is supported for the reconciliation file is CSV. For more information, see the topic "Example comma-separated value (CSV) file" in the *IBM Security Identity Manager Administration Guide*.

12. Click **Finish**.

Results

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

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table and display the new service instance.

Changing services

You can change the information for a service instance.

Before you begin

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

Before you can change a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To change a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, select the check box next to the service that you want to change, and then click **Change**.
4. On the Service Information or General Information page, change the appropriate values for the service instance, and then click **OK**.
5. On the Access Information page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable. Clearing the check box disables these fields. Change any access information or any other optional information such as description, search terms, more information, or badges.

Results

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

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Changing connection mode from manual to automatic

After installing the adapter, you can automate the routing of account requests to the managed resource.

Before you begin

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

Before you can change a service, you must create the service instance with connection mode. The corresponding adapter for the managed resource must also be installed. For more information about enabling connection mode and creating a service with connection mode, see these topics:

- "Enabling connection mode" on page 120
- "Creating a service that has manual connection mode" on page 117

About this task

Use connection mode to change the account request routing from manual to automatic. You do not have to delete a manual service or create a service for the adapter.

Note: If you have pending work orders prior to switching the connection mode, a popup message reminds you. Use the **View Activities** option to resolve requests that are already in the activity list. After the switch to automatic, complete reconciliation to sync with the end point. Alternately, use the **View Requests by Service** option to cancel any current requests on the service. You can resolve the requests either before or after changing to automatic connection mode. After the change to automatic connection mode, the managed resource handles all new account requests.

Procedure

To change the connection mode for a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.

d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, select the check box next to the service that you want to change, and then click **Change**.
4. On the Service Information or General Information page, change the connection mode from manual to automatic. Then click **Test Connection** to validate that the data in the fields is correct. If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

   Note: The content of the Service Information or General Information page depends on the type of service that you are changing.
5. Change any other appropriate values for the service instance, and then click **OK**.

Results

A message is displayed, indicating that you successfully changed the service instance. The managed resource handles all account requests.

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Changing a manual service

Change information for a manual service instance.

Before you begin

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

Before you can change a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To change a manual service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether the search must be done against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, select the check box next to the manual service that you want to change, and then click **Change**.
4. On the General Information page, change the appropriate values for the service instance, and then click **Participants**.
5. On the Participants page, change the participants type, escalation time in days, or escalation participant type.
6. Optional: On the Messages page, complete these steps, and then click **Reconciliation**:
   a. Select the email message that you want to change, and then click **Change**. The Change Message page is displayed.
   b. Modify the **Subject** and **Body** fields as wanted, and then click **OK**.
7. Optional: On the Reconciliation page, click **Browse** to locate the reconciliation file, and then click **Upload File** to load the new reconciliation file. You can also choose whether to reconcile supporting data only.

   Note: The file type supported for the reconciliation file is CSV. For more information, see the topic "Example comma-separated value (CSV) file" in the *IBM Security Identity Manager Planning Guide*.
8. Click **OK** to save the changes and to close the page.

Results

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

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Values and formats for CSV access data (service)

A service access CSV file can contain multiple values and supported formats.

Consider these points before you work with any CSV files for a service access:

- If you use a custom label for AccessType, specify the key in the CSV file.
- If you use a custom label for badge text, add a $ prefix on the key. For example, $mail.
- Define multiple values for search terms and badges with a semicolon (;) separator.
- Define the AccessType hierarchy with a colon (:) separator.
- Use the badgeText~badgeStyle format for badges.

Define CSV columns for a service, group, or a role access as follows:

Table 8. CSV fields and values. CSV fields and values

Field name	Value
SERVICE_DN, SERVICE_NAME	Not modifiable.
DEFINE_AS_ACCESS	TRUE or FALSE. If you do not assign any value, then FALSE is assumed.
ACCESS_NAME	Required for services and groups, and contains a maximum length of 240 characters. This field is not available for roles.
ACCESS_TYPE	Required. You must specify an access type that is defined in IBM Security Identity Manager.

Table 8. CSV fields and values (continued). CSV fields and values

Field name	Value
ACCESS_DESCRIPTION	Contains a maximum length of 240 characters.
ICON_URL	Provide a valid icon URL value on the access definition.
SEARCH_TERMS	Each search term contains a maximum length of 80 characters. You can have multiple search terms.
ADDITIONAL_INFORMATION	Contains a maximum length of 1024 characters.
BADGES	The maximum length for each badge text is 512 characters. You can have multiple badges. The badge text that is prefixed with a $ sign cannot contain delimiter characters such as ., ;, =, or white space.

A service access CSV file for an export or import operation in the IBM Security Identity Manager administration console contains these columns with sample values and supported formats:

Table 9. Part 1 of 2: Service access CSV file values, formats

SERVICE_NAME	DEFINE_AS_ACCESS	ACCESS_NAME	ACCESS TYPE	ACCESS_DESCRIPTION	ICON_URL
admin	TRUE	Access	Application:Finance	This access is for the admin service.	/itim/ui/custom/ui/images/homepage/RequestAccess.png
AIX Service	FALSE	AIX Service	Application:Finance:Payroll	This access is for the AIX Service.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg
Default Service	TRUE	default access	MailService	This access is a default service access.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg

Table 10. Part 2 of 2: Service access CSV file values, formats

SERVICE_NAME	SEARCH_TERMS	ADDITIONAL_INFORMATION	BADGES	SERVICE_DN
admin	Service Access; Manager	Service that is used by a client user.	admin~green	erglobalid=562867050689119980 3,ou=services,erglobalid=000000
AIX Service	Employee;Service;AccessService	Used by the customer to deploy server.	$roleaccess~red	erglobalid=562866975213090286 9.ou=services,erglobalid=000000
Default Service	Mail;Unique ID	BVT server that is used to run BVT from developer and tester.	$mail~green;Risky~red	erglobalid=562867033703021524 5,ou=services,erglobalid=000000

Exporting access data for a service

Export the access data for a service in a comma-separated value (CSV) file format by using the IBM Security Identity Manager Console.

Before you begin

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

Before you export a service, you must have ACI privileges for `Modify Operation` on the service that you want to view. If the necessary privileges do not exist, then the service is not exported.

The **Export Access Data** button is not active until you select some service accesses to activate it. Only the service access that you selected is exported as access data.

About this task

Export the selected service access data in a CSV file format for your requirements.

Procedure

1. From the navigation tree, select **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, in the **Services** table, click **Export Access Data**. The Export access data page is displayed. After you submit the export request, a process status indicates the advancement of the export operation.
3. Optional: Click **Cancel** to discontinue the export operation.

4. Click **Download Exported File** to download the CSV file on your local system by using your web browser settings. The exported CSV file contains all the service access data.

   Note: Click **Download Export Log File** to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Results

The exported CSV file contains all the access data for a service. Click **Close** to exit from the Export access data page.

What to do next

Import access data for a service, or you can continue to export access data by clicking **Export Access Data** in the Select a Service page.

Importing access data for a service

Use the IBM Security Identity Manager Console to import the service access data from a comma-separated value (CSV) file.

Before you begin

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

The privileged user that uploads the CSV file must have the appropriate permissions.

Before you import a service, you must have ACI privileges for `Search Operation` and `Modify Operation` on the service that you want to update. If the necessary privileges do not exist, then the service is not imported.

Before you import a CSV file, verify that the CSV-related conventions are met. They are as follows:

- The access type hierarchy is represented in the following format, and each access type be separated by a colon (`:`). For example:

  ```
  AccessType1:AccessType2
  ```

- The badge information is provided in the following format. For example:

  ```
  badgeText~badgeStyle
  ```

- Multiple badges can be assigned to accesses in the following format, and each badge must be separated by a semicolon (`;`). For example:

  ```
  Badge1~red;Badge2~green
  ```

- Multiple search terms and access types can be specified by using the semicolon (`;`) separator.
- The relevant keys must be provided in the CSV file for the customized labels that are related to badges and access types.

About this task

Only the accesses with the **Define as Access** set to `True` are defined as accesses, and the corresponding data is imported.

Procedure

1. From the navigation tree, select **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, in the **Services** table, click **Import Access Data**. The Import access data page is displayed.
3. Click **Browse** in **File to Upload (.CSV)** to locate and upload a valid CSV file that contains all the access data for a service.
4. Click **Import** to import the CSV file. After you submit the import request, a process status indicates the advancement of the import operation.

   Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

   If any problems occur when you are importing a CSV file, then close the Import access data page to continue working with the IBM Security Identity Manager Console. The problems might be due to one of the following conditions:

   - The access data CSV file does not exist.
   - The CSV file was renamed.
   - The CSV file does not contain appropriate separators or delimiters.
5. Optional: Click **Cancel** to discontinue the import operation.

   Note: Click **Download Import Log File** to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Results

The imported CSV file contains all the access data for a service. Click **Close** to exit from the Import access data page.

What to do next

Export access data for a service, or you can continue to import access data by clicking **Import Access Data** in the Select a Service page.

Configuring access catalog information for a service

Configure the access catalog information for a service in the Administrator Console so you can use it in the Identity Service Center Request Access workflow.

Before you begin

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

You must create a service type before you can configure the access catalog information for a service in IBM Security Identity Manager.

You can also configure the access catalog information for an existing service.

About this task

Configure the access information for a service by defining certain accesses with the use of a badge. You can highlight certain accesses with badges by attaching text that contains some formatting such as color and font type.

Procedure

To configure the service access information, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, click **Create** to display the Create a Service wizard. Alternatively, select an existing service and click **Change** to configure its access catalog information.
3. Specify appropriate values in the corresponding tabbed pages.
4. On the Access Information page, complete these steps to configure the access information:
   a. Select the **Define an Access** check box to activate the access definition fields.
   b. Specify an appropriate name in the **Access name** field.
   c. Expand the **Select access type** or the **Change access type** tree to select an access type. The tree label depends on whether you want to create or modify a service.
   d. Provide a uniform resource identifier (URI) string in the **Icon URL** field for the access icon.
   e. Specify search strings in the **Search terms** field to return specific search terms. Add or delete the search terms to suit your requirements.
   f. Specify any free form information about the access item in the **Additional information** field.
   g. Expand the **Badges** section to specify the badges that are associated with the role.
      - Specify a badge text in the **Badge text** field.
      - Assign a class from the **Badge class** list for the badge text.

      You can see the preview of your badge specifications in the **Preview** area.
5. Depending on whether you created or modified the service access information, click **OK** or **Finish** when you are done.

Results

The access information is added or updated to the service object and stored in the Security Identity Manager LDAP server.

What to do next

On the Success page, click **Close**.. Select another services task, or click **Close**.

Deleting services

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

Before you begin

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

Before you can delete a service in IBM Security Identity Manager, a service instance must exist.

Procedure

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, select the check box next to the service that you want to remove, and then click **Delete**. Selecting the check box at the top of this column selects all service instances. A confirmation page is displayed.
4. On the Confirm page, click **Delete** to remove the selected service instance, or click **Cancel**. The services are removed automatically from all provisioning policies, identity policies, password policies, adoption policies, and recertification policies that currently reference them. If all services referenced by a policy are deleted by this operation, the entire policy is also deleted. All accounts that are related to that service are also deleted from Security Identity Manager. However, they are not de-provisioned from the managed resource.

Results

A message indicates that you successfully deleted the service instance.

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Management of reconciliation schedules

Reconciliation is the process of synchronizing the accounts and supporting data to the IBM Security Identity Manager Server central data repository from a managed resource. Reconciliation is required when accounts and supporting data can be changed on the managed resource so that IBM Security Identity Manager Server data is consistent and up-to-date with the remote resource.

During the reconciliation process, new accounts created on the managed resource will be created in the IBM Security Identity Manager Server repository and assigned to the user based on the adoption policy that is applicable for the service.

If there is no user match for the account, the account will be displayed in IBM Security Identity Manager Server as an orphan account that can be manually assigned to a user by a IBM Security Identity Manager Server administrator. Modified accounts on the managed resource will be updated to the IBM Security Identity Manager Server repository. Removed accounts on the managed resource are also removed from IBM Security Identity Manager Server.

You can manage schedules for reconciliation, or initiate a reconciliation activity immediately. To determine an ownership relationship, reconciliation compares account information with existing user data stored on the IBM Security Identity Manager Server by first looking for the existing ownership within the IBM Security Identity Manager Server and, secondly, applying adoption rules configured for the reconciliation.

If there is a match of user login IDs to an account, the IBM Security Identity Manager Server creates the ownership relationship between the account and the person. The IBM Security Identity Manager Server also verifies that the accounts fit within the constraints of a defined policy. If there is not a match, the IBM Security Identity Manager Server lists the unmatched accounts as orphaned accounts.

You run reconciliation to perform the following tasks:

- Load accounts and account supporting data information, including groups, into IBM Security Identity Manager

  Promptly after IBM Security Identity Manager is installed, you should submit reconciliation requests for all resources whose accounts are managed by IBM Security Identity Manager. Reconciliation inserts accounts from the managed resources into the IBM Security Identity Manager directory.
- Monitor accesses granted outside of IBM Security Identity Manager

  During reconciliation, records of all accesses granted outside of IBM Security Identity Manager are inserted into the IBM Security Identity Manager directory. You can view these records by user after your data is reconciled.

  Reconciliation allows you to enable policy checking. In this case, you should reconcile your data on a scheduled basis for your organization's ongoing security audits.

Managed service accounts can be excluded from reconciliation on the IBM Security Identity Manager Server and, for some adapters, on the managed service itself. If you filter accounts from reconciliation at the adapter and do not also filter them when you define your server-side scheduled or immediate reconciliations, the server will consider the reconciliation a "full" reconciliation for all accounts and will remove any accounts from its directory that it does not receive during the reconciliation (because it will appear to the server that they have been removed from the managed resource).

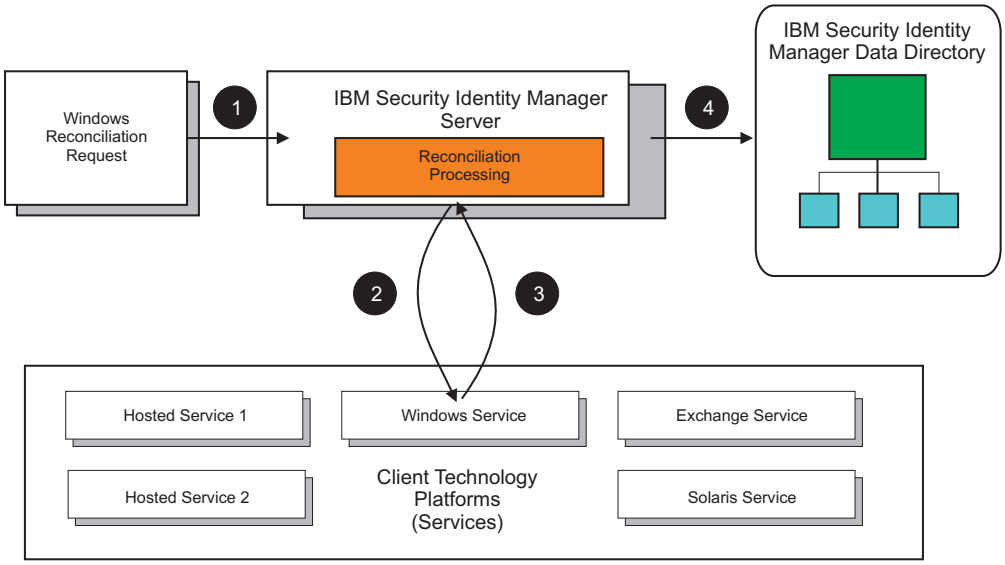
Consider the following best practices for using reconciliation:

- Perform supporting data reconciliation separately from accounts. The separation is useful during initial deployment for the service and also useful for sync up changes of metadata without accounts, which is very time-consuming. Supporting data includes group configuration information, which contains key information about access privileges on the resource. Bringing back the group data ahead of time allows policies to be configured promptly before accounts are reconciled, so that the policies can be enforced.

- Set up reconciliation schedules appropriately based on the frequency of data changes. Leave enough time between two reconciliations. Avoid unnecessary reconciliations.
- Queries are used to break reconciliation into smaller packets. Reconcile only the data that is changed by using Query. Reconciliation is an expensive process, especially when policy checking is enabled.
- If you are working with a large data repository (that is, a large number of accounts), consider using Query to segment the data and perform the reconciliation in smaller chunks on different schedules.
- Specify a subset of account attributes to bring back to improve performance.

Overview of the reconciliation process

The following illustration is an overview of the reconciliation process. In this example, IBM Security Identity Manager reconciles Windows Server data.



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

Step	Description
1	An administrator submits a reconciliation request to a system whose security is managed by IBM Security Identity Manager.
2	The IBM Security Identity Manager Server sends the reconciliation request to the selected service.
3	The service collects information from the system and sends the information to the IBM Security Identity Manager Server.
4	The IBM Security Identity Manager Server reads the information and reconciles the IBM Security Identity Manager directory with account information from the service.
5	The IBM Security Identity Manager Server attempts to find the account owner.
6	If an owner is found, the changes to the account are evaluated against a provisioning policy.
7	The account is modified according to configured policy enforcement options.

Reconciling accounts immediately on a service

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

Before you begin

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

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

To prevent the reconciliation from running again at the scheduled time, change or delete the scheduled reconciliation.

Procedure

To run a reconciliation now, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Reconcile Now**. The tasks that you can perform are dependent on the type of service. The Select Query page is displayed.
4. Select one of the following options:
   - **None**. Select this option to include all accounts in the reconciliation.
   - **Use query from existing schedule**. Select this option to view and select reconciliation from an existing schedule.
   - **Define query**. Select this option if you want to allow the reconciliation to filter accounts that fit the selected attributes, or if you want to perform a "supporting data only" reconciliation.
5. Click **Submit** to request an immediate reconciliation activity.

Results

A message is displayed, indicating that you successfully submitted a reconciliation request to run immediately.

What to do next

To view the results of the reconciliation, click **View the status of the reconciliation request**, or click **Close**.

Creating a reconciliation schedule

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

Before you begin

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

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

Procedure

To create a reconciliation schedule, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Set Up Reconciliation**. The tasks that you can do are dependent on the type of service. The Manage Schedules page is displayed.
4. On the Manage Schedules page, complete the following steps:
   a. Specify whether a policy evaluates the accounts that the reconciliation returns.
   b. Click **Create**. The Set Up Account Reconciliation notebook is displayed.
5. On the General page, type information about reconciliation schedule.
6. On the Schedule page, select a schedule interval for the reconciliation. The fields displayed depend on the scheduling option that you select.
7. Optional: On the Query page, specify that you are doing a "supporting data only" reconciliation, which brings back only metadata for accounts and excludes accounts. Alternatively, use the LDAP filter to specify the subset of accounts or specific type of support data such as a group to be included in the reconciliation. Specify the subset of account attributes to bring back during the reconciliation. By default, IBM Security Identity Manager brings back all attributes of accounts. By specifying the subset of attributes that is likely to be changed on the remote resource, you can improve reconciliation performance.

8. Click **OK** to save the new schedule and close the page.

Results

A message is displayed, indicating that you successfully created a reconciliation schedule.

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Changing a reconciliation schedule

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

Before you begin

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

A reconciliation schedule must exist.

Procedure

To change a reconciliation schedule, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Set Up Reconciliation**. The tasks that you can do are dependent on the type of service. The Manage Schedules page is displayed.
4. On the Manage Schedules page, complete the following steps:
   a. Specify whether a policy evaluates the accounts that the reconciliation returns.
   b. On the Manage Schedules page, select the check box next to the reconciliation schedule that you want to modify, and then click **Change**. The Set Up Account Reconciliation notebook is displayed.
5. Make the wanted changes on the General, Schedule, and Query pages, and then click **OK**.

Results

A message is displayed, indicating that you successfully updated an existing reconciliation schedule.

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Deleting a reconciliation schedule

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

Before you begin

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

A reconciliation schedule must exist.

Procedure

To delete a reconciliation schedule, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Set Up Reconciliation**. The tasks that you can do are dependent on the type of service. The Manage Schedules page is displayed.
4. On the Manage Schedules page, select the check box next to the reconciliation schedule that you want to delete. Selecting the check box at the top of this column selects all reconciliation schedules.
5. Click **Delete** A confirmation page is displayed.
6. On the Confirm page, click **Delete** to delete the selected reconciliation schedule, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the reconciliation schedule.

What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Configuring a manual service type to support groups

To support group assignment, but not group management for manual services, the group profile needs to be set up in the manual service type configuration.

Before you begin

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

About this task

To set up a manual service type to support group assignment, but not group management (which includes create, read, update, delete) for manual services, complete these steps:

Procedure

1. Define the group schema as an LDAP objectclass in the IBM Security Identity Manager LDAP server.
2. Define a manual service (complete with service and account objectclasses). The account objectclass should contain an optional multi-valued attribute that will be used to store the group membership information. This service type should reference the group schema created in the previous step.

   The Manage Service Types page allows the administrator to select an existing LDAP objectclass for use as the group schema class. If you want to create a new objectclass, you must create it manually and load it directly into the LDAP server.

   The mapped **Group ID**, **Group name**, and **Group description** attributes can all reference the same group schema attribute, if desired. You cannot define multiple groups that use the same group ID. The ID must be unique per group.

   More than one group schema can be defined for a given service type. The definition of the second and subsequent schemas is performed in the same manner as the first.
3. Modify service and account forms for the service type using the form designer. This step is required to properly display needed information when creating the service instance as well as creating accounts.
4. Create a manual service instance using the manual service type that you created earlier in this process.

Reconciling accounts immediately on a service

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

Before you begin

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

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

To prevent the reconciliation from running again at the scheduled time, change or delete the scheduled reconciliation.

Procedure

To run a reconciliation now, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Reconcile Now**. The tasks that you can perform are dependent on the type of service. The Select Query page is displayed.
4. Select one of the following options:
   - **None**. Select this option to include all accounts in the reconciliation.
   - **Use query from existing schedule**. Select this option to view and select reconciliation from an existing schedule.
   - **Define query**. Select this option if you want to allow the reconciliation to filter accounts that fit the selected attributes, or if you want to perform a "supporting data only" reconciliation.
5. Click **Submit** to request an immediate reconciliation activity.

Results

A message is displayed, indicating that you successfully submitted a reconciliation request to run immediately.

What to do next

To view the results of the reconciliation, click **View the status of the reconciliation request**, or click **Close**.

Example comma-separated value (CSV) file

Create a CSV file for reconciliation of the manual service instance. The CSV file contains both accounts and group definitions that exist on the manual service.

Using a CSV file for reconciliation of a manual service

Here is an example CSV file that contains both account and group information:

```
eruid,description
batman,uses technology
superman,flies through the air
spiderman,uses a web
ghostrider, rides a motorcycle
#GROUP_OBJECT_PROFILE#accessgroupGroupProfile
cn,description
daredevil,this group represents daredevils
superhero,this group represents superheroes
```

The example file creates two groups for this service instance: `daredevil` and `superhero`. Because `cn` is used for both the `id` and `name` attributes in the group schema, list it only one time in the CSV file. The example file also creates four accounts for this service instance: `batman`, `superman`, `spiderman`, and `ghostrider`.

Format of the example CSV file

The first line of the example CSV file contains the attribute header list for accounts. The list contains the attributes that are defined in the accounts section of the service type definition. Be sure to include any required attributes in this line, or else the reconciliation fails.

The next set of lines (up until the `#GROUP_OBJECT_PROFILE#` line) represents the accounts that are to be loaded into IBM Security Identity Manager. Each line represents one account. The content of these rows is the values to apply to the attributes defined in the first row. All required attributes must have a value, or else the reconciliation of that account fails.

The line that starts with `#GROUP_OBJECT_PROFILE#` is a line that delineates the start of a new group schema (as defined in the **Manage Service Types** task). The string immediately after `#GROUP_OBJECT_PROFILE#` is the name of the group schema as stored in IBM Security Identity Manager. The value is always *`objectclass`*`GroupProfile`. In the example file, the `accessgroup` objectclass is used for the group schema, so the value for this line is `accessgroupGroupProfile`. If this line does not reference an existing group profile in IBM Security Identity Manager, the reconciliation fails.

The line immediately following the `#GROUP_OBJECT_PROFILE#` line is the group header line that lists the attributes of the group that is defined on the previous line. This line should contain the three attributes defined on the Groups page of the **Manage Service Types** task.

Following the example, the values are the group id, group name, and group description: `cn`, `cn`, `description`. If these attributes do not exist in the group profile, the reconciliation fails. Include any attribute that exists in the group schema objectclass that you defined, but only the group name and group description appear in the IBM Security Identity Manager interface.

The next group of lines represents individual groups of the group schema type. Each line represents one group. The values listed on this line correspond to the attribute list on the line immediately following the `#GROUP_OBJECT_PROFILE#` line. If the values on this line are not valid, then the creation of that group in IBM Security Identity Manager fails when the reconciliation is done.

Example CSV file for loading two types of group profiles

More than one type of group can be loaded by using the reconciliation file. To do so, repeat the #GROUP_OBJECT_PROFILE# line in the CSV file. Here is an example that loads two types of group profiles:

```
eruid,description
batman,uses technology
superman,flies through the air
spiderman,uses a web
ghostrider, rides a motorcycle
#GROUP_OBJECT_PROFILE#accessgroupGroupProfile
cn,description
daredevil,this group represents daredevils
superhero,this group represents superheroes
#GROUP_OBJECT_PROFILE#aixaccessgroupGroupProfile
aixgroupadminlist,ibm-aixprojectnamelist,ergroupdescription
eadmins,eadmingroup,admins on ephone
eguests,eguestgroup,guests on ephone
```

The two group schemas used in this example are `accessgroup` and `aixaccessgroup`. For the reconciliation to work, both group schemas must be defined on the service type.

Reconciling supporting data only

When you do the reconciliation, you can select a check box for *supporting data only*. If you select the check box, the reconciliation ignores the account information and processes only the group information. If you do not select the check box, both account and group information is processed. The CSV file can contain both accounts and groups, groups only, or accounts only. The reconciliation ignores missing data.

Management of accounts on a service

An *account* is an entity that contains a set of parameters that define the application-specific attributes of a user, including the identity, user profile, and credentials.

An account defines your login information, such as your user ID and password, and your access to the specific resource with which it is associated.

In IBM Security Identity Manager, accounts are created on account types. The types represent the managed resources such as operating systems (such as UNIX), applications (for example, Lotus Notes), or other resources. An account type is defined as part of the service type for the managed resource. The account type contains the account profile object that describes the schema of an account and mapping of account attributes to IBM Security Identity Manager-managed account attributes.

Accounts are either active or inactive. Accounts must be active to log in to the system. An account becomes inactive when it is suspended or if a request to recertify your account usage is declined and the recertification action is suspend. Suspended accounts still exist, but they cannot be used to access the system.

If one of your accounts is inactive and you require access to the system, contact your system administrator to restore the account.

Displaying accounts on a service

You can display the accounts that are associated with the service instance.

Before you begin

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

Before you can display accounts on a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To display accounts on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Accounts**. The tasks that you can do are dependent on the type of service. The Accounts page is displayed.
4. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.

      Note: When you select an ownership of type `Individual` from the list to search accounts, the search yields a list of accounts with ownership of types `Individual` and `None`.

Results

A list of accounts that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the accounts in the **Accounts** table, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Requesting accounts on a service

You can submit a request for an account on a service or schedule submission of the request.

Before you begin

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

Before you can request accounts on a service in IBM Security Identity Manager, you must create a service instance. In addition, the user must already be provisioned for an account on the service.

Procedure

To request an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Request Accounts**. The tasks that you can do are dependent on the type of service. The Select a User page is displayed.
4. On the Select a User page, complete these steps:
   a. Type information about the user in the **Search information** field.
   b. In the **Search by** list, select the criteria that you want, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of users that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. Select the user that you want to request an account for, and then click **Continue**. The Select an Ownership Type page is displayed.
6. Select the ownership type for the account, and then click **Continue**. The Account Information page is displayed.

7. Specify information for the account, including whether to change the password at the next login, and then click one of the following buttons:
   - **Submit Now**. This option submits the account request immediately.
   - **Schedule Submission**. This option opens the Schedule page. Specify whether to schedule the request immediately, or specify the date and time for submitting the account request, and then click **Submit**.

Results

A message is displayed, indicating that you successfully submitted a request to create an account on the service.

What to do next

Select another account request task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Changing accounts on a service

You can change an account on an existing service if necessary.

Before you begin

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

Before you can change accounts on a service in IBM Security Identity Manager, you must create a service instance.

In addition, an account must exist, and the account must have an owner. In other words, orphan accounts cannot be changed.

Procedure

To change an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Accounts**. The tasks that you can do are dependent on the type of service. The Accounts page is displayed.
4. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.

b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

5. In the **Accounts** table, select the check box next to the account that you want to change, and then click **Change**. The Account Information page is displayed.
6. Change information for the account, and then click **Submit Now** or **Schedule Submission**. The schedule submission option opens a new page where you can specify the date and time for submitting the changes to the account.

Results

A message is displayed, indicating that you successfully submitted a request to change an account on the service.

What to do next

Select another account task, or click **Close**. When the Accounts page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Deleting accounts from a service

You can delete an account from a service instance if necessary.

Before you begin

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

Before you can delete accounts from a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To delete an account from a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Accounts**. The tasks that you can do are dependent on the type of service. The Accounts page is displayed.
4. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, select the check box next to the account that you want to delete, and then click **Delete**. Selecting the check box at the top of this column selects all accounts. A confirmation page is displayed.
6. On the Confirm page, specify the date and time for the deletion to occur, and then click **Delete**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to delete an account from the service.

What to do next

Select another account task, or click **Close**. When the Accounts page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Suspending accounts on a service

You can suspend an account on a service. This action makes the account inactive.

Before you begin

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

Before you can suspend accounts on a service in IBM Security Identity Manager, you must create a service instance.

In addition, an account must exist, and the account must have an owner.

Note: Suspension of an account does not automatically terminate active sessions that use the suspended account. The account owner is notified when the account is suspended. For privileged accounts that have special privileges to access sensitive information in the system or application, the account owner must follow up manually to ensure that the suspended account can no longer be used to access the system or application immediately after the account is suspended.

Procedure

To suspend an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Accounts**. The tasks that you can do are dependent on the type of service. The Accounts page is displayed.
4. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, select the check box next to the account that you want to suspend, and then click **Suspend**. A confirmation page is displayed.
6. On the Confirm page, specify the date and time for the suspension to occur, and then click **Suspend**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to suspend an account on the service.

What to do next

Select another account task, or click **Close**. When the Accounts page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Restoring accounts on a service

You can restore an inactive account on a service and make the account active again.

Before you begin

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

Before you can restore accounts on a service in IBM Security Identity Manager, you must create a service instance.

The account must be inactive, and it must have an owner.

Procedure

To restore an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Accounts**. The tasks that you can do are dependent on the type of service. The Accounts page is displayed.
4. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, select the check box next to the account that you want to suspend, and then click **Restore**. The Schedule page is displayed.
6. On the Schedule page, specify the date and time for the restoration to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to restore an account on the service.

What to do next

Select another account task, or click **Close**. When the Accounts page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Assigning an account to a user

You can assign an account to a user.

Before you begin

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

You must create a service instance and do a reconciliation.

Procedure

To assign an account to a user, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Accounts**. The tasks that you can do are dependent on the type of service. The Accounts page is displayed.
4. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, click the icon (▸) next to the account to show the tasks that can be done on the account, and then click **Assign to User**. The Select a User page is displayed.
6. On the Select a User page, complete these steps:

a. Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
b. In the **Users** table, select the name of the user that you want to assign the selected account to, and then click **Continue**. If the provisioning policy entitles more than one ownership type, the Select an Ownership Type page is displayed. Otherwise a confirmation page is displayed.

7. On the Select an Ownership Type page, choose an ownership type for the account. The provisioning policy for the service determines the number of ownership types available. This page is displayed only if more than one ownership type is entitled on the service. A confirmation page is displayed.
8. On the Confirm page, specify the date and time for the account assignment to occur, and then click **Assign to User**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to assign an account to a user.

What to do next

Select another account task, or click **Close**. When the Accounts page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Orphan accounts

Orphan accounts are accounts on the managed resource whose owner in the IBM Security Identity Manager Server cannot be determined.

Orphan accounts are identified during reconciliation when the applicable adoption rule cannot successfully determine the owner of an account. You can also make an account into an orphan account if the current owner of the account is not correct.

Orphan accounts are included in the list of accounts that are associated with a service. You can suspend or delete orphan accounts or assign them to users.

- When you assign an orphan account to a user, the user becomes the owner of the account. Also, the policies that are applicable to the users are evaluated and enforced for the account. The owner can manage the account with the Self Service or the Identity Service Center user interface.
- When you suspend an orphan account, it is suspended on the Security Identity Manager Server and on the managed resource.
- When you delete an orphan account, it is deleted on the managed resource.

Making an orphan account

You can change an account so that it is an orphan account.

Before you begin

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

You must create a service instance and either created an account or done a reconciliation on an existing account.

Procedure

To change an account so that it is an orphan account, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Accounts**. The tasks that you can do are dependent on the type of service. The Accounts page is displayed.
4. On the Accounts page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether the search is to be done against user IDs or owners.
   c. In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, click the icon (▸) next to the account to show the tasks that can be done on the account, and then click **Orphan**. A confirmation page is displayed.
6. On the Confirm page, specify the date and time for the orphan operation to occur, and then click **Orphan**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to change an account to an orphan account.

Note: When an account becomes an orphan account, it no longer has an ownership type. Provisioning policies do not apply to orphan accounts.

What to do next

Select another account task, or click **Close**. When the Accounts page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Management of account defaults on a service

You can define default values for account attributes either on a service or on a service type.

Note: In previous versions of IBM Security Identity Manager, account defaults were specified with provisioning policy. Account defaults differ from a provisioning policy. Account defaults do not define the set of users who are allowed to have accounts or what attribute values are compliant. Defaults define the default values for a new account. The change of account default configuration does not affect the compliance status of user accounts. A service might be granted for a subset of users (for example, users who belong to specific organization roles). In this case, these global account defaults might be duplicated in multiple provisioning policies that are specific for each role. By using account defaults, you avoid duplicated configurations.

The following list highlights the differences between the use of account defaults and provisioning policies:

- Like "default" provisioning parameters, account defaults specify the default values for account attributes during provisioning.
- Unlike "default" provisioning parameters, account defaults are not scoped by membership. They apply to all users.
- Unlike "default" provisioning parameters, account defaults do not have implications on compliance. A value specified as an account default is not automatically treated as an "allowed" value.
- Values that are specified as account defaults do not occur within the entitlement parameter list. They are entirely independent from provisioning policy.
- Provisioning parameters take precedence over account defaults. Specifically, mandatory and default provisioning parameters override an account default for the same attribute.

Here is an example to illustrate the differences. In this example, we want to define default values and compliance around the "Local Groups" attribute of WinLocal accounts.

In one case, Case A, we define the default value as a provisioning parameter. In the other case, Case B, we define the default value as an account default.

- Case A:

  Default provisioning parameter
  Guests

  Allowed provisioning parameter
  Print Operators

- Case B:

  Account default
  Guests

  Allowed provisioning parameter
  Print Operators

In both cases, its clear that **Print Operators** is an allowed value for the attribute. It is also true that in both cases the default value for the attribute is **Guests**. The difference is that defining the value of **Guests** as a provisioning parameter in Case A makes **Guests** an allowed value. An account with **Local Groups = Guests** is

compliant. In Case B, an account with **Local Groups = Guests** is not compliant because account default values do not have any implications on compliance.

Consider the following tips for using Account Defaults instead of Provisioning Policy:

- Use account default to set up default account values for attributes that do not affect security concerns. Use provisioning policy to set up account attribute constraints for security compliance. Avoid using the same attributes for both purposes.
- Use default parameters in provisioning policy to set up default values for security sensitive attributes. The defaults can be automatically given to a user when the account is created.
- Use allowed parameters or exclude all but the wanted parameters in provisioning policy to grant access privilege to a user.
- Use mandatory parameters in a provisioning policy to support "required" (must have) access privilege for a user. IBM Security Identity Manager ensures that these values are set for new account. The values are out to an existing account when policy enforcement is set to `correct` and `alert`.

Adding account defaults to a service

You can add default values for attributes. When you create an account for this service, the default values are provided.

Before you begin

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

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

Consider doing a "supporting data only" reconciliation to sync up account metadata before you configure the account defaults.

About this task

If account defaults are already defined on the service type for this service, a message is displayed. It indicates that account defaults are defined for the service type. If you click **OK**, then the account defaults for the service type are copied to the service. You can either change the account defaults on the service or remove them from the service. Any changes (including removals) do not affect the account defaults on the service type.

Procedure

To add account defaults to a service, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.

d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Account Defaults**. The tasks that you can do are dependent on the type of service. The Select an Account Attribute page is displayed.
4. On the Select an Account Attribute page, click **Add** to add an attribute. The Select an Attribute to Default page is displayed.
5. On the Select an Attribute to Default page, select an account attribute, and then click one of the following options:
   - **Add**, to add a default value for the selected attribute. Complete the appropriate fields, which vary depending on the type of service, and then click **OK**. The attribute default is added to the list on the Select an Attribute to Default page.
   - **Add (Advanced)**, to add a script that specifies a default value for the selected attribute. Type the JavaScript code in the **Script** field, and then click **OK**. The attribute default is added to the list on the Select an Attribute to Default page.
6. On the Select an Account Attribute page. When you are finished adding attribute defaults to the service instance, click **OK** to save the changes and to close the page. For JavaScript APIs that are available for account defaults, see the JavaScript document and look for JavaScript Extensions for host component "Account Default."

Results

A message is displayed, indicating that you successfully saved the account defaults on the service.

What to do next

Select another account task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Changing account defaults for a service

You can change the account defaults for a service instance.

Before you begin

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

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

About this task

You can change the default values for attributes. The changed default values will **not** affect existing accounts but will be used for new accounts that are created on the service.

Procedure

To change account defaults for a service, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) adjacent to the service to show the tasks that can be done on the service, and then click **Account Defaults**. The tasks that you can do are dependent on the type of service. The Select an Account Attribute page is displayed.
4. On the Select an Account Attribute page, select the check box adjacent to the attribute that you want to modify, and then click one of the following options:
   - **Change**, which allows you to change the default value for the selected attribute. Complete the appropriate fields, which vary depending on the type of service, and then click **OK**. The template value for the attribute is updated in the list on the Select an Attribute to Default page.

     Note: If you select this option when an attribute currently has a scripted default value, the existing script will be overwritten with the template value that you specify.
   - **Change (Advanced)**, which allows you to add or change a script that specifies a default value for the selected attribute. Type the wanted JavaScript code in the **Script** field, and then click **OK**. The template value for the attribute is updated in the list on the Select an Attribute to Default page.
5. On the Select an Account Attribute page, when you are finished changing attribute defaults for the service instance, click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully saved the account defaults on the service.

What to do next

Select another account task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Removing account defaults from a service

You can remove account defaults from a service instance.

Before you begin

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

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

About this task

Account defaults for the service type are used.

Procedure

To remove account defaults from a service, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Account Defaults**. The tasks that you can do are dependent on the type of service. The Select an Account Attribute page is displayed.
4. On the Select an Account Attribute page, select the check box next to the attribute that you want to remove, and then click **Remove**. Selecting the check box at the top of this column selects all attributes. The attribute default is removed from the list on the Select an Attribute to Default page.
5. On the Select an Account Attribute page, finish removing attributes from the service instance. Click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully removed the account defaults from the service.

What to do next

Select another account task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Using global account defaults for the service type

Instead of adding account defaults to a service instance, you can use the global account defaults for the service type.

Before you begin

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

About this task

Selecting this option prevents new account defaults from being created on the service, and prevents existing account defaults from being changed or removed. The **Add**, **Change**, and **Remove** buttons are disabled when you choose to use global account defaults.

Procedure

To use the global account defaults for the service type, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Account Defaults**. The tasks that you can do are dependent on the type of service. The Select an Account Attribute page is displayed.
4. On the Select an Account Attribute page, select the check box for **Use the global account defaults for the service type**, and then click **OK**. The buttons and attributes on the Select an Account Attribute are disabled.
5. On the Select an Account Attribute page, click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully saved the account defaults on the service.

What to do next

You can choose to use the account defaults instead of using the global account defaults by clearing the **Use the global account defaults for the service type** check box on the Select an Account Attribute page.

Select another account task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Service tagging

A service tag is used for grouping services. Security Identity Manager, starting with Version 6.0, provides an *ertag* attribute to the service objects. With this attribute, you can group services of the same type by tagging them together. Because the *ertag* attribute is a multi-value attribute, a service can have one or more service tags. Services with the same service tag belong to the same group of services.

The provisioning policies are enhanced to support the service tag entitlement. A service tag entitlement is a service type entitlement with one or more tags. It applies to all services of the specified type with at least one matching tag. For example, if a service tag entitlement might be defined for a Linux service type with the service tag *mytag1* and *mytag2*. Only services of the Linux type that are tagged with either *mytag1* or *mytag2* are subject to the provisioning policy entitlement. Or, if two service tag entitlements are defined as *mytag1* and *mytag2*, then a service with both tags is subject to both entitlements.

A service type entitlement is different from a service tag entitlement in a way that it applies to all services of the specified type. For example, when managing a provisioning policy, you might select POSIX AIX profile as the service type without adding any service tags. All AIX services that you create are governed by this provisioning policy, regardless of whether they have tags or not.

When the service tag attribute is modified, accounts can become noncompliant. You must use Enforce policy on a service task to reevaluate all policies that govern the service. The policy enforcement gathers all policies that affect the selected service, reevaluates the existing accounts, and provisions new accounts.

It is important to understand that the Change service operation does not automatically start policy enforcement. You must manually enforce policies on the service.

Adding the tag attribute to the service template

About this task

Follow these steps to configure the service template.

Procedure

1. Log on to the Security Identity Manager administrative console.
2. From the navigation tree, click **Configure System** > **Design Forms**. The form designer applet opens.
3. In the left pane, double-click the **Service** folder to open the object profiles for the service types available.
4. Double-click the wanted object profile. For example, POSIX AIX profile, to open the template for that profile. The form template that is associated with the object profile, that is, POSIX AIX profile, is opened in the middle pane.
5. Select the tab to which you want to add the tag attribute. For example, `$servicetabgeneral`.
6. In the Attribute List pane on the right, double-click the `ertag` attribute. The tag attribute is added to the form.

7. To add a multi-value tag attribute, follow these steps:
   a. Right-click **[TextField]** of `$ertag` from the middle pane.
   b. Select **Change to** > **Editable Text List**. **[TextField]** becomes **[Editable Text List]**.
8. Click **Form** > **Save Form Template** > **OK** to save the new template.

Adding tags to the service

When you have the tag attribute ready in the service template form, you can add tags to the services.

About this task

Follow these steps to add the tags.

Procedure

1. Log on to the Security Identity Manager administrative console.
2. From the navigation tree, click **Manage Services**.
3. Click **Create** from the Services table. The Create Service page opens.
4. Select the type of the service, for example, POSIX AIX profile, and then click **Next**.
5. Specify information about a service instance.
6. In the **Tag** field at the bottom of the page, type the name of the tag and click **Add**. Add more tags when necessary, for example, mytag1, mytag2.
7. Proceed to finish creating a service.

Policy enforcement

Policy enforcement reevaluates accounts to determine whether they violate provisioning policies.

Provisioning policies govern the access rights of users for specific services. Provisioning enforcement is incorporated into all business processes that manage the identities and access rights of users on a managed resource. *Policy enforcement* performs appropriate actions to ensure that user access rights comply with the corporate policies.

Policy enforcement is automatically triggered when you create, modify, or delete the provisioning policies. The following table lists the activities that can automatically start policy enforcement.

Class	**Operations**
Account	Create, modify, delete, request account
Service Group	Request access
Service	Configure policy enforcement, reconcile
Provisioning policy	Change policy
Role	modify membership

However, you must manually start policy enforcement when:

- You create a new service.
- You tag a service or change a service tag.

These situations can cause accounts to become noncompliant or require new accounts to be provisioned. The policies governing this service must be reevaluated to ensure that all accounts are compliant with the provisioning policies. If policy enforcement finds any missing accounts for users who are automatically entitled to an account, it provisions new accounts for them.

You can configure policy enforcement globally or for a specific service. You can choose these enforcement actions:

- Mark
- Suspend
- Correct
- Alert
- Use Global Enforcement: Mark

All services except DSML Identity Feed services have policy enforcement. You can perform policy enforcement at any time. When you select to enforce a policy, policy enforcement is scheduled to take action.

Policy enforcement actions

To resolve noncompliant accounts on a service, you can take one of these actions:

Mark Flags the disallowed account or an account that has noncompliant attribute value.

Suspend
Deactivates the disallowed account or an account that has noncompliant attribute value.

Correct
Replaces a noncompliant attribute on an account with the correct attribute.

The disallowed accounts from the policy evaluation can be exempt from this **Correct** action. IBM Security Identity Manager provides the default exemption handler. This handler uses the `correct.enforcement.exemption.account.criteria` property in the `enRole.properties` file to determine the matching criteria of exempt accounts. The accounts that match any of the specified criteria are orphaned instead of being removed. The exempt action is defined by the `correct.enforcement.exemption.account.action` property value specified in the `enRole.properties` file.

You can also plug in your own custom exemption handler. You can implement the `com.ibm.itim.policy.dynanalysis.ICorrectEnforcementExemptionHandler` Java Interface and specify the implementation class name in the `correct.enforcement.exemption.account.handler` property of the `enRole.properties` file. For more information about the Java interface and writing your own exemption handler, see the API documentation.

Alert Notifies the user about a disallowed account or value.

Use Global Enforcement Action: Mark
Uses the current global enforcement action for a noncompliant account value.

Policy enforcement alerts

Policy enforcement alerts notify a dedicated user about security compliance violations so that they can correct them. When an account becomes noncompliant, the person designated in the compliance alert configuration is notified. To make a noncompliant account compliant, a service owner can then create a compliance process for Security Identity Manager to bring the account back into compliance.

Depending on the privilege rules defined on the account attributes, accounts are considered noncompliant when users:

- Possess account privileges for reasons that are no longer valid.

  In this situation, you must revoke the privileges to make the accounts compliant. When privileges are revoked, you must define a compliance process for policy enforcement. When the policy enforcement action is set as **Alert**, the compliance alert process is triggered.
- Do not possess account privileges that they must have.

  In this situation, you must grant privileges to these users to make the accounts compliant. If an account is noncompliant because additional privileges are needed, those privileges are granted automatically.

When you define a compliance process to enforce a policy, the noncompliant accounts are flagged. Separate compliance alert items are generated for each privilege to be revoked for each account. For example, if an account has two groups that violate the provisioning policies, you address these two groups separately. You can remove one group while you can add a policy to the other group to make it compliant. Different people can perform these corrective actions at different times.

Two types of operations can trigger policy enforcement:

- System-triggered operations, also called indirect operations. They include service reconciliation, policy change, and identity change operations.
- Manually triggered operations, also called direct operations. They include the operations performed directly or manually on an account.

The following actions might trigger a policy enforcement action:

- Changing a policy.
- Performing a service reconciliation.
- Changing an identity in the user interface or through an identity feed. You can revoke privileges through dynamic role changes or entitlement parameter recalculation based on identity information.
- Adding a role to a user.
- Removing a role from a user.
- Changing the definition for a dynamic role.
- Manually modifying an account.

The following table shows the default compliance alert settings.

Table 11. Default compliance alert settings

Operation type	Check box status	Required changes	Action taken for		Account state	Request state
			Granting changes	Revoking changes		
System-triggered	**Checked**	Granting	Added	-	Compliant	Success
		Revoking	-	Alerted	Noncompliant	#
		Both	Added	Alerted	Noncompliant	#
		None	-	-	Compliant	Success
	UNCHECKED**	Granting	Added	-	Compliant	Success
		Revoking	-	Removed	Compliant	Success
		Both	Added	Removed	Compliant	Success
		None	-	-	Compliant	Success
Manually triggered	**Checked**	Granting	Alerted	-	Noncompliant	#
		Revoking	-	Alerted	Noncompliant	#
		Both	Alerted	Alerted	Noncompliant	#
		None	-	-	Compliant	Success
	UNCHECKED**	Granting	Exception*	-	Same as previous state	Failed
		Revoking	-	Exception*	Same as previous state	Failed
		Both	Exception*	Exception*	Same as previous state	Failed
		None	-	-	Compliant	Success

Notes:

* Generates the workflow exception `CREATE_ACCOUNT_IS_DISALLOWED`.

** `UNCHECKED` results in the same behavior as selecting `Correct` as the enforcement action.

The request remains in the `Pending` state until the compliance process completes.

Compliance alerts

When a change to an account causes privileges to be revoked, the system can generate a compliance alert and send it to a designated user. The **Compliance Alert To Do** item in the compliance alert contains information about the noncompliant account. The recipient of the alert can either accept or reject some or all of the changes to this account.

Configuring policy enforcement behavior

You can configure the policy enforcement behavior for accounts that do not comply with existing provisioning policies.

Before you begin

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

Before you can configure policy enforcement behavior on a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To configure the policy enforcement behavior, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Configure Policy Enforcement**. The tasks that you can do are dependent on the type of service. The Select Action page is displayed.
4. On the Select Action page, select an enforcement action:
   - Select **Mark** to mark a disallowed account or an account that has a noncompliant attribute value, and then click **Continue**.
   - Select **Suspend** to suspend an account that is disallowed or that has noncompliant attribute values, and then click **Continue**.
   - Select **Correct** to remove an account or replace noncompliant attributes on an account with the correct attributes, and then click **Continue**. Disallowed accounts can be exempt from this action if they meet the criteria of exempt accounts, which is defined in the `enRole.properties` file. See *Policy enforcement actions* in "Policy enforcement" on page 159.
   - Select **Alert** to issue an alert for an account that is disallowed or that disallows attribute values (revoking attribute values), and then click **Continue**.
   - Select **Use Global Enforcement Action** to use the current global enforcement action for an account that has a noncompliant attribute, and then click **Continue**.
5. On the Confirm page, specify the date and time for the enforcement action to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully saved the policy enforcement settings for the service.

What to do next

View the status of the request, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Configuring compliance alert rules

Configure compliance alert rules to specify when compliance alerts are sent.

Before you begin

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

Before you can configure policy enforcement behavior on a service in IBM Security Identity Manager, you must create a service instance.

About this task

Security Identity Manager must make an informed decision about which account change operations are granting additional privileges and which are revoking privileges for noncompliance resolution. This decision allows users to be informed about accounts that are disallowed or privileges to be revoked before Security Identity Manager removes it from the user. For multi-valued attributes, Security Identity Manager accomplishes this choice through a simple subset relation. For single-valued attributes, Security Identity Manager consults privilege rules to differentiate between granting and revoking actions.

If no privilege rules are defined for an attribute, then any change in a single-valued attribute is assumed to be a revoke action that leads to creation of a compliance alert.

Procedure

To configure compliance alert rules, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Configure Policy Enforcement**. The tasks that you can do are dependent on the type of service. The Select Action page is displayed.
4. On the Select Action page, select **Alert**, and then click **Continue**. The Configure Policy Enforcement Behavior notebook is displayed.
5. On the **General** tab of the notebook, complete the following steps:
   a. In the **Alert name** field, type a descriptive name for the alert.
   b. Select the participants to receive the alerts. The participant fields vary, depending on the type of participants you select.

c. Specify the time intervals.
d. Select the process types for which an alert is generated. If no process type is selected, the system automatically corrects a noncompliant account for that process type. The correction can modify or delete the account.

6. Optional: On the **E-mail** tab of the notebook, either use the default template, or provide text for the alert notification email message.
7. Click **Submit**. A confirmation page is displayed.
8. On the Confirm page, specify the date and time for the enforcement action to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully saved the policy enforcement settings for the service.

What to do next

View the status of the request, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Enforcing policies

When a service is tagged or a service tag changes, use this task to reevaluate the governing provisioning policies for the service.

Before you begin

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

Reconcile the new service before you enforce policies. Enforcing policies on a new service without reconciling first might cause enforcement errors.

Procedure

To schedule policy enforcement on a service, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that you can do on that service.
4. Click **Enforce Policy**. The tasks that you can do depend on the type of service. The Schedule page is displayed.

5. Select either **Immediate** or **Effective date** to schedule the policy enforcement.
6. Click **Submit**.

Results

A message indicates that you successfully submitted a request to enforce policy on the service.

Account recertification

You can view the status of recertification on accounts, or override the recertification rejection status for accounts.

Account recertification is a process that is used to determine whether accounts are still needed. If the accounts are still needed, then more justification might be required. If the accounts are no longer needed, then certain actions need to be taken. System administrators can create recertification policies for all services, while service owners can create recertification policies for services they own.

All services other than the identity feed service are eligible for recertification. A service can be a member of only one recertification policy.

Orphaned accounts are not included for recertification targets.

You can view the latest recertification status of accounts by service instance.

The administrator or service owner can override certain recertification rejection actions by recertifying accounts on a service. Suspended accounts are not reactivated during the recertification process. The override actions are logged in the recertification log table for reporting.

Displaying account recertification status

You can display the recertification status for accounts that are associated with the service instance.

Before you begin

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

Before you can display account recertification status on a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To display the recertification status for accounts on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.

c. Select a service type from the **Search type** list.
d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Account Recertification Status**. The tasks that you can do are dependent on the type of service. The Account Recertification Status page is displayed.
4. On the Account Recertification Status page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether to search against user IDs or owners, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify more search criteria.

Results

A list of accounts that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the accounts in the **Account Recertification Status** table, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Recertifying accounts on a service

You can manually recertify accounts that are associated with the service instance. You can also override the recertification status of the account on the service.

Before you begin

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

Before you can recertify accounts on a service in IBM Security Identity Manager, you must create a service instance.

About this task

Accounts that have a rejection status or that are not certified and that can be overridden, have a check box.

Procedure

To recertify the accounts on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Account Recertification Status**. The tasks that you can do are dependent on the type of service. The Account Recertification Status page is displayed.
4. On the Account Recertification Status page, complete these steps:
   a. Type information about the account in the **Account information** field.
   b. In the **Search by** field, specify whether to search against user IDs or owners, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
5. In the **Account Recertification Status** table, select the check box next to the account that you want to recertify, and then click **Recertify**. Selecting the check box at the top of this column selects all accounts. A confirmation page is displayed.
6. On the Confirm page, type a reason for the recertification in the **Justification** field, and then click **Recertify**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully overrode the recertification status of the account on the service.

What to do next

Select another recertification task, or click **Close**. When the Account Recertification Status page is displayed, click **Refresh** to refresh the **Account Recertification Status** table, and then click **Close**.

Management of groups or access on a service

You can define access, manage group membership, or view the recertification status for the group. Groups are supported in most services managed by IBM Security Identity Manager to allow sets of users to be administered collectively for access control purposes.

Access privileges to IT resources are based on membership of a group. In IBM Security Identity Manager Version 4.6, groups were treated as one of the supporting data on the managed service. Group membership was an attribute on an account. In IBM Security Identity Manager Version 5.0 and there after, groups are treated as supporting data. Groups are also a new type of entity in the IBM Security Identity Manager model. In addition, access that is represented by a group is made available for users to directly request.

Administrators can do these management functions for groups and accesses:

- Review the groups on the managed service
- Assign members to a group or remove members from a group
- Provide business-friendly names, categories, and descriptions of the access represented by the group
- Expose the access to users so that users can directly request or remove access
- Specify owners of access and specify approval of group access requests
- Define policies to enforce the recertification of group access

When access information for the group is defined and enabled in the access view, group membership affects the access list for a user. When a user is added to a group, the access that is granted to the user is displayed in the user's access list. When a user is removed from a group, the access is revoked from the user and removed from the access list.

Approval process for groups and accesses

The approval process might be different for managing groups or accesses, depending on how the request is initiated and submitted. When you manage group members from the Manage Services task, the request is treated as *account* request. Therefore, the request goes through the *account* approval. If the same group is exposed as an access and is requested through an *access* request, then the request goes through the *access* approval. The request does not go through account approval. Only when there is no access approval defined, the request continues to use account approval.

Define access for a group

A service owner can provide business-friendly names, categories, and descriptions of the access represented by the group. The service owner can expose the access to users so that users can directly request or remove access. Service owners can specify the owner of the access, the approval process for the access, and the notification options for access provisioning.

Access types

The following access types are included with IBM Security Identity Manager:

- Application
- Shared Folder
- Mail Group
- Role

Groups on a service are defined with supporting data. The relevant target group information is reconciled as supporting data, which uses a filtered reconciliation on the associated service on the target, pulling back only the groups. The access itself is then defined from groups on a service.

The definition of each access is a one-to-one mapping with a group defined for the adapter type.

After an access is provisioned, the requester effectively becomes a member of the group who is defined by the access entitlement on the target. For access, this reconciliation of supporting data is critical. After the groups are reconciled, access definitions can be created.

Access owner
Access owner is a dedicated IBM Security Identity Manager user who is responsible for the access. ACIs can be set up to grant privileges on the access for the owner. The access owner is often involved in the approval process.

Access approval
Access approval specifies the access request workflow for access request. The access request workflow is defined with the **Access Request Workflow** task. Typically, this workflow is used to define the approval process for the access request.

Access notification
Access notification defines whether the email notifications are sent to the user when access is provisioned or de-provisioned for them.

Clearing access

You can clear an access from its association with the service instance.

Before you begin

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

Before you can clear access on a service in IBM Security Identity Manager, you must create a service instance.

About this task

This task allows the service owner to clear the access definition for a group.

Procedure

To clear access from a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon (▸) next to the service to show the tasks that can be done on the service, and then click **Manage Groups**. The tasks that you can do are dependent on the type of service. The Manage Groups on Service page is displayed.
4. On the Manage Groups page, complete these steps:
   a. Type information about the group in the **Group information** field.
   b. In the **Search by** field, specify whether to search against groups or accesses, and then click **Search**. A list of groups or access that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Groups** table, select the group that has the access that you want to clear, and then click **Change**.
5. On the General Information page:
   a. Click the **Access Information** tab to display the Access Information page.
   b. Clear the **Define an Access** check box to clear the access and all its data.
   c. Click **OK** to submit your changes.

Results

A list of groups or access that matches the search criteria is displayed. The access information for the group is cleared, and the group is not exposed in the access request.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the items in the **Group** table, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Chapter 9. Group administration

IBM Security Identity Manager provides predefined groups. You can also create and modify customized groups.

Creating groups

You can create groups either on the ITIM Service or on managed resources.

Before you begin

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

If a new group requires a new business unit, create the business unit first. To limit group activities, you might create an extra view or access control item after you create a group. You might create an access control item on the ITIM Service before creating a group. If the group does not previously exist, the access control item does not have the intended membership.

You might upgrade from IBM Tivoli Identity Manager version 5.0 to version 5.1 and use a service instance that was created with a IBM Tivoli Identity Manager 5.0 profile. If so, you must upgrade to the 5.1 adapter before you create groups on the service.

About this task

You can use the Create Group wizard to create more groups.

Procedure

To create a group, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the Create Group wizard, complete these steps:
   a. On the Select Type page, click the radio button next to the type of group that you want to create, and then click **Next**. The Select Type page is displayed only if the service supports more than one type of group.

b. On the General Information page, complete the expected fields. Click **Next** to display the Access Information page, or click **Finish** to complete the operation without adding access information or any members to the group.
c. Optional: On the Access Information page, select the **Define an Access** check box to activate the access definition fields. Click the radio button for the type of access you want to enable. Specify the expected access information and any other information such as access type, description, access owner, search terms, approval workflow, notification options, search terms, or badges. Click **Next** to display the Group Membership page, or click **Finish** to complete the operation without adding any members to the group.
d. Optional: On the Group Membership page, add members to the group, and then click **Next** to display the Schedule Add Member Operation page.
e. On the Schedule Add Member Operation page, specify when to add the members to the group, and then click **Finish**. The Schedule Add Member Operation page is displayed only if you chose to add members to the group on the Group Membership page.

Results

A page is displayed, indicating that the operation was successful. The new group is created on the service.

What to do next

You can create another group, add or remove members for the new group, or click **Close** to close the page.

If the new group is created on the ITIM Service, you can create an access control item to associate with this group.

Viewing group membership

You can view members of groups.

Before you begin

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

Procedure

To view members of a group, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. On the Select Group page, complete these steps to view the groups that exist for the service:
   a. Type information about the group in the **Search information** field.

      For ITIM service groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.

      For managed resource groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

      A list of groups that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

4. In the **Groups** table, click the icon (▸) next to the group, and then click **Manage Members**. The Manage Members page is displayed.
5. On the Manage Members page, complete these steps:
   a. Type information about the user in the **System account information** field.
   b. In the **Search by** field, specify whether the search is done against users or user IDs, and then click **Search**.

Results

A list of users that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

You can add or remove group membership.

Adding members to groups

You can add members to groups.

Before you begin

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

Procedure

To add members to a group, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. On the Select Group page, complete these steps to view the groups that exist for the service:
   a. Type information about the group in the **Search information** field.

      For ITIM service groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.

      For managed resource groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

      A list of groups that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
4. In the **Groups** table, click the icon (▸) next to the group, and then click **Add Members**. The Add Members page is displayed.
5. On the Add Members page, complete these steps:
   a. Type information about the user in the **System account information** field.
   b. In the **Search by** field, specify whether the search is done against users or user IDs, and then click **Search**. A list of users that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
   c. In the **System Accounts** table, select one or more users that you want to add to the group, and then click **OK**. A confirmation page is displayed.
6. On the Confirm page, specify when you want the users to be added to the group, and then click **Submit**. A page is displayed, indicating that the operation was successful.
7. On the Success page, click **Close**.

Results

The members are added to the group.

What to do next

You can continue working with groups, add or remove more members, or view your request.

Removing members from groups

You can remove members from groups.

Before you begin

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

Procedure

To remove members from a group, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. On the Select Group page, complete these steps to view the groups that exist for the service:
   a. Type information about the group in the **Search information** field.

      For ITIM service groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.

      For managed resource groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

      A list of groups that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
4. In the **Groups** table, click the icon (▸) next to the group, and then click **Manage Members**. The Manage Member page is displayed.
5. On the Manage Members page, complete these steps:
   a. Type information about the user in the **System account information** field.

b. In the **Search by** field, specify whether the search is done against users or user IDs. Then, click **Search**. A list of users that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

c. In the **Group Membership** table, select one or more users that you want to remove from the group, and then click **Remove**. A confirmation page is displayed.

6. On the Confirm page, specify when you want the users to be removed from the group, and then click **Remove**. A page is displayed, indicating that the operation was successful.
7. On the Success page, click **Close**.

Results

The members are removed from the group.

What to do next

You can continue working with groups, add or remove more members, or view your request.

Modifying groups

As an administrator, you can modify the attributes of a group. These attributes depend upon the type of service that you selected for the group.

Before you begin

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

Determine what expansion or limits to set on the tasks the members see, and, which access control items might also require changes.

You cannot change the predefined System Administrator group.

Procedure

To change a group, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search Type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. On the Select Group page, to view the groups that exist for the service, type the information about the group in the **Search information** field.

   For ITIM service groups
   In the **Search by** field, specify whether the search is done against group name or descriptions, or business units and then click **Search**.

   For managed resource groups
   In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

   A list of groups that match the search criteria is displayed.

   If the table contains multiple pages, you can:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

4. In the **Groups** table, select the group that you want to modify, and then click **Change**. The Change Group page is displayed.
5. On the Change Group page, take the following actions:

   ITIM service groups
   To Change the view, select the wanted view from the **View** menu. Type or change a description in the **Description** field. When your changes are made, click **OK** to complete the operation.

   Managed resource groups
   The fields that are displayed and that can be modified depend on the type of remote service you selected.

   Note: Although the **Group ID number** is a modifiable field, do not change this number because doing so compromises system security. After you modify the information, click the **Access Information** tab to display the Access Information page, or click **OK** to complete the operation without changing access information. On the Access Information page, you can modify the information such as access type, description, owner, search terms, approval workflow, notification options, search terms, or badges. Then, click **OK** to complete the operation.

Results

A page is displayed, indicating that the group change operation was successful. The changes that you made to the group are now in effect.

What to do next

On the Success page, click **Close**.

Values and formats for CSV access data (group)

A group access CSV file can contain multiple values and supported formats.

Consider these points before you work with any CSV files for a group access:
- If you use a custom label for AccessType, specify the key in the CSV file.

- If you use a custom label for badge text, add a $ prefix on the key. For example, $mail.
- Define multiple values for search terms and badges with a semicolon (;) separator.
- Define the AccessType hierarchy with a colon (:) separator.
- Use the badgeText~badgeStyle format for badges.

Define CSV columns for a group access as follows:

Table 12. CSV fields and values. CSV fields and values

Field name	Value
GROUP_DN, GROUP_NAME	Not modifiable.
DEFINE_AS_ACCESS	TRUE or FALSE. If you do not assign any value, then FALSE is assumed.
ACCESS_NAME	Required for services and groups, and contains a maximum length of 240 characters. This field is not available for roles.
ACCESS_TYPE	Required. You must specify an access type that is defined in IBM Security Identity Manager.
ACCESS_DESCRIPTION	Contains a maximum length of 240 characters.
ICON_URL	Provide a valid icon URL value on the access definition.
SEARCH_TERMS	Each search term contains a maximum length of 80 characters. You can have multiple search terms.
ADDITIONAL_INFORMATION	Contains a maximum length of 1024 characters.
BADGES	The maximum length for each badge text is 512 characters. You can have multiple badges. The badge text that is prefixed with a $ sign cannot contain delimiter characters such as ., ;, =, or white space.

A group access CSV file for an export or import operation in the IBM Security Identity Manager administration console contains these columns with sample values and supported formats:

Table 13. Part 1 of 2: Group access CSV file values, formats

GROUP_NAME	DEFINE_AS_ACCESS	ACCESS_NAME	ACCESS TYPE	ACCESS_DESCRIPTION	ICON_URL
admin	FALSE	Access	Application:Group	This access is for the admin group.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg
AIX Group	TRUE	AIX Group	AccessGroup	This access is for the AIX group.	/itim/ui/custom/ui/images/homepage/RequestAccess.png
Default Group	TRUE	default access	EmailGroup:Department:Location	This access is a default group access.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg

Table 14. Part 2 of 2: Group access CSV file values, formats

GROUP_NAME	SEARCH_TERMS	ADDITIONAL_INFORMATION	BADGES	SERVICE_DN
admin	Group;Group access	Group that is used by a client user.	$highrisk~red	erglobalid=562867050689119980 3,ou=groups,erglobalid=000000
AIX Group	Employee;Group;AccessGroup	Used by the customer to deploy server.	Group~yellow	erglobalid=562866975213090286 9,ou=groups,erglobalid=000000
Default Group	Mail;Unique ID	BVT server that is used to run BVT from developer and tester.	$mailer~yellow;highrisk~red	erglobalid=562867033703021524 5,ou=groups,erglobalid=000000

Exporting access data for a group

Export the access data for a group in a comma-separated value (CSV) file format by using the IBM Security Identity Manager Console.

Before you begin

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

Before you export a group, you must have ACI privileges for `Define Access` and `Search Operations` on the group that you want to view. If the necessary privileges do not exist, then the group is not exported.

The **Export Access Data** button is not active until you select some group accesses to activate it. Only the group access that you selected is exported as access data.

About this task

Export the selected group access data in a CSV file format for your requirements.

Procedure

1. From the navigation tree, select **Manage Groups**. The Select Group page is displayed.
2. On the Select Group page, in the **Groups** table, click **Export Access Data**. The Export access data page is displayed. After you submit the export request, a process status indicates the advancement of the export operation.
3. Optional: Click **Cancel** to discontinue the export operation.
4. Click **Download Exported File** to download the CSV file on your local system by using your web browser settings. The exported CSV file contains all the group access data.

   Note: Click **Download Export Log File** to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Results

The exported CSV file contains all the access data for a group. Click **Close** to exit from the Export access data page.

What to do next

Import access data for a group, or you can continue to export access data by clicking **Export Access Data** in the Select Group page.

Importing access data for a group

Use the IBM Security Identity Manager Console to import the group access data from a comma-separated value (CSV).

Before you begin

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

The privileged user that uploads the CSV file must have the appropriate permissions.

Before you import a group, you must have ACI privileges for `Search`, `Define Access`, and `Modify Operations` on the group that you want to update. If the necessary privileges do not exist, then the group is not imported.

Before you import a CSV file, verify that the CSV-related conventions are met. They are as follows:

- The access type hierarchy is represented in the following format, and each access type be separated by a colon (`:`). For example:

  ```
  AccessType1:AccessType2
  ```

- The badge information is provided in the following format. For example:

  ```
  badgeText~badgeStyle
  ```

- Multiple badges can be assigned to accesses in the following format, and each badge must be separated by a semicolon (;). For example:
  `Badge1~red;Badge2~green`
- Multiple search terms and access types can be specified by using the semicolon (;) separator.
- The relevant keys must be provided in the CSV file for the customized labels that are related to badges and access types.

About this task

Only the accesses with the **Define as Access** set to `True` are defined as accesses, and the corresponding data is imported.

Procedure

1. From the navigation tree, select **Manage Groups**. The Select Group page is displayed.
2. On the Select Group page, in the **Groups** table, click **Import Access Data**. The Import access data page is displayed.
3. Click **Browse** in **File to Upload (.CSV)** to locate and upload a valid CSV file that contains all the access data for a group.
4. Click **Import** to import the CSV file. After you submit the import request, a process status indicates the advancement of the import operation.

   Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

   If any problems occur when you are importing a CSV file, then close the Import access data page to continue working with the IBM Security Identity Manager Console. The problems might be due to one of the following conditions:
   - The access data CSV file does not exist.
   - The CSV file was renamed.
   - The CSV file does not contain appropriate separators or delimiters.
5. Optional: Click **Cancel** to discontinue the import operation.

   Note: Click **Download Import Log File** to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Results

The imported CSV file contains all the access data for a group. Click **Close** to exit from the Import access data page.

What to do next

Export access data for a group, or you can continue to import access data by clicking **Import Access Data** in the Select Group page.

Deleting groups

You can delete groups from an ITIM service or from a managed resource.

Before you begin

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

Before you delete a group, remove the members from the group, and remove the reference to the group from provisioning policy entitlement parameters.

About this task

You cannot delete a group that has members. If you delete a group that is referenced by provisioning policies, you must remove those references from the provisioning policy parameters. Otherwise, those references might generate warnings for the affected accounts. For ITIM Service groups, members who are logged on during removal from a group continue to have their current tasks. The change in group membership takes effect at the next logon.

Procedure

To delete a group, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. On the Select Group page, complete these steps to view the groups that exist for the service:
   a. Type information about the group in the **Search information** field.

      For ITIM service groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.

      For managed resource groups
      In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list and then click **Search**.

      A list of groups that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
4. In the **Groups** table, select one or more groups that you want to delete, and then click **Delete**. A confirmation page is displayed.

5. On the Confirm page, click **Delete**. A page is displayed, indicating that the delete operation was successful.

Results

The group is deleted from the service.

What to do next

You can continue working with groups, or click **Close**.

Defining access on a group

Define an access to be associated with the group.

Before you begin

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

Before you can display groups or access on a service in IBM Security Identity Manager, you must create a service instance. In addition, you must do a supporting data reconciliation on that service.

About this task

This task enables the service owner to define access information for a group.

Procedure

To display the groups or access on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. On the Select Group page, to view the groups that exist for the service, type the information about the group in the **Search information** field. In the **Search by** field, specify whether to search against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

   A list of groups that matches the search criteria is displayed.

   If the table contains multiple pages, you can:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

4. In the **Groups** table, select the group for which you want to define an access and then click **Change**. The Change Group page is displayed.
5. On the General Information page, complete these steps:
   a. Click the **Access Information** tab to display the Access Information page.
   b. Select the **Define an Access** check box to activate the access description fields.
   c. Select the radio button for the type of access you want to enable.
   d. Specify an access name in the **Access name** field.
   e. Specify other information such as icon url, search terms, or badges.
   f. When you are finished, click **OK**.

Results

A page is displayed, indicating that the group change operation was successful. The access information is added to the group object and stored in the Security Identity Manager LDAP server. If the access is enabled, the user can search and request the access.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

On the Success page, click **Close**.

or you can select to:

- Manage groups on a different service
- Return to the list of groups that you were working with

Configuring access catalog information for a group

Configure the access catalog information for a group in the Administrator Console so you can use it in the Identity Service Center Request Access workflow.

Before you begin

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

You must create a service instance before you can configure the access catalog information for a group in IBM Security Identity Manager.

You can also configure the access catalog information for an existing group.

About this task

Configure the access information for a group by defining certain accesses with the use of a badge. You can highlight certain accesses with badges by attaching text that contains some formatting such as color and font type.

Procedure

To configure the group access information, complete these steps:

1. From the navigation tree, click **Manage Groups**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. Specify appropriate values in the corresponding tabbed pages
4. On the Access Information page, complete these steps to configure the access information:
   a. Select the **Enable access for this group** check box.
   b. Specify the name, access type, access description, owner, approval, notification options for the group.

      You can also specify the icon for the access, search terms, additional information, and badges which are used in the Identity Service Center Request Access.
   c. Expand the **Select access type** or the **Change access type** tree to select an access type. The tree label depends on whether you want to create or modify a service.
   d. Provide a uniform resource identifier (URI) string in the **Icon URL** field for the access icon.
   e. Specify search strings in the **Search terms** field to return specific search terms. Add or delete the search terms to suit your requirements.
   f. Specify any free form information about the access item in the **Additional information** field.
   g. Expand the **Badges** section to specify the badges that are associated with the role.
      - Specify a badge text in the **Badge text** field.
      - Assign a class from the **Badge class** list for the badge text.

      You can see the preview of your badge specifications in the **Preview** area.
5. Depending on whether you created or modified the group access information, click **OK** or **Finish** when you are done.

Results

The access information is added or updated to the group object and stored in the Security Identity Manager LDAP server.

What to do next

On the Success page, click **Close**. You can also do the following actions:

- Manage groups on a different service

- Return to the list of groups that you were working with
- Create another group, add, or remove members for the new group
- Create an access control item to associate with this group if the new group is created on the Security Identity Manager service.

Recertifying access on a group

Recertify an access to be associated with the group.

Before you begin

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

Before you can recertify access on a group in IBM Security Identity Manager, you must create a service instance. In addition, you must do a supporting data reconciliation on that service.

About this task

This task allows the service owner to view the recertification status of user access for the selected group. This task also allows the service owner to overwrite the recertification status for access that is either `Never Certified` or `Rejected`.

Procedure

To recertify access on a group, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Search information** field.
   b. In the **Search by** field, specify whether to search against services or business units.
   c. Select a service type from the **Search type** list.
   d. Select a status from the **Status** list, and then click **Search**. A list of services that matches the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. Type information about the group in the **Search information** field. In the **Search by** field, specify whether to search against group names or descriptions, or access name, select a type of group from the **Group type** list, and then click **Search**. A list of groups that matches the search criteria is displayed.

   If the table contains multiple pages, you can:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
4. In the **Groups** table, click the icon (▸) next to the group for you want to manage, and then click **Access Recertification Status**. The Access Recertification Status page is displayed.

5. In the **Access Recertification Status** table, select the check box next to the access that you want to recertify, and then click **Recertify**. Selecting the check box at the top of this column selects all accesses. A confirmation page is displayed.

Results

A list of groups or access that matches the search criteria is displayed. After the recertify operation is complete, the access in the list is marked as `Certified`.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the items in the **Groups** table, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Enabling automatic group membership

You can set whether automatic membership occurs in a service owner or manager group.

Before you begin

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

About this task

You can use the Set Security Properties page to automatically put the IBM Security Identity Manager accounts of newly named service owners or managers in their groups.

To create a group, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Set Security Properties**.
2. On the Set Security Properties page, in the **Group Settings** section, select the **Automatically populate Identity Manager groups** check box, and then click **OK**. A page is displayed, indicating that the operation was successful.

Results

The automatic action is enabled or disabled immediately. If it is enabled, the Security Identity Manager accounts of newly named managers are placed in the default Managers group.

You do not need to restart the Security Identity Manager Server.

What to do next

On the Success page, click **Close**.

Chapter 10. Report administration

IBM Security Identity Manager provides reports for system activity, resources such as accounts that users own, and historical data.

Overview

A *report* is a summary of IBM Security Identity Manager activities and resources. You can generate reports based on requests, user and accounts, services, or audit and security. You can also design custom reports with the report designer.

Report data is staged through a data synchronization process. The process gathers data from the IBM Security Identity Manager directory information store and prepares it for the reporting engine. Data synchronization can be run on demand, or it can be scheduled to occur regularly.

The generated reports are based on the most recent data synchronization, not on current data. Activities that occur after the last data synchronization was done are captured by the next data synchronization. Data in the reports is obtained from the IBM Security Identity Manager database and the directory server.

Access control is available for report management. There are default ACIs for the Manager, Service Owner, and Auditor groups. For example, service owners and managers can search for all persons that they can access. Managers can see direct reports, and service owners can see people on services controlled by ACIs. Auditors can run all reports and see all data. No report access is available for users or members of the Help Desk group.

To generate a report, you must synchronize data at least one time. The report data is based on the most recent data synchronization and is only as accurate as the report data from that synchronization.

Reports are displayed in a separate window; therefore, you must disable pop-up blocking in your browser in order for the reports to be displayed. When you generate a report, be sure to close the report window in your browser before you generate another report. If you do not close the open report window before generating another report, a message displays, instructing you to close the window. Or, the same report might be displayed if it was cached by the browser.

Note: Complex report structures and report query requirements mandate that recertification reports are implemented in Java code rather than in Structured Query Language (SQL). Complex structures include Recertification History, Accounts/Access Pending Recertification and Recertification Policies reports.

Report formats

You can generate reports as a PDF file or as a comma-separated value (CSV) file. By default, reports are generated in PDF format and can be viewed and printed with the Adobe Acrobat Reader. In some cases, PDF formatting produces an additional blank page at the end of the report, which does not indicate that data is missing. You might select a CSV file for the report output. The report is displayed

with the application that is mapped to CSV files (for example, Microsoft Excel). If no application is associated with the CSV file type, you are prompted to open or save the file when the report is created.

A PDF report, by default, can contain up to 5000 records. You can change this value with the `enrole.ui.report.maxRecordsInReport` property in the `UI.properties` file. You do not have to restart the server for the changes to take effect. Changes can occur between 30 seconds and 10 minutes. You can increase this value to obtain larger amounts of data in your reports. However, it is possible that you might encounter an `OutOfMemoryError` error by doing so. If this error occurs, increase the application server heap size in the WebSphere Application Server and restart IBM Security Identity Manager.

Report accessibility
The Security Identity Manager reports are accessible in the PDF format.

IBM Cognos reporting framework

Security Identity Manager version 6.0 provides the Cognos® reporting framework to create and analyze reports. You can modify the schema and generate reports in different formats.

Note:

Security Identity Manager version 6.0.0.6 supports IBM Cognos Business Intelligence Server, version 10.2.1 as well as version 10.2.2. By default, the Security Identity Manager version 6.0.0.6 report package is packaged with IBM Cognos Business Intelligence Server, version 10.2.1.

Reports in the IBM Cognos Business Intelligence Server, version 10.2.1 can run in the IBM Cognos Business Intelligence Server, version 10.2.2. However, if you work with IBM Cognos Business Intelligence Server, version 10.2.2, the compatibility with an earlier versions of IBM Cognos Business Intelligence Server is not supported. For more information about installation and configuration of IBM Cognos Business Intelligence Server, version 10.2.2, see http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.2/com.ibm.swg.ba.cognos.cbi.doc/welcome.html?.

Note: Cognos reporting does not support Microsoft SQL Server database. Use DB2 database or Oracle database instead.

The IBM Cognos reporting framework includes the following items:

Reporting model
Represents the business view of Security Identity Manager data. You can use the models to customize and generate different types of reports that suit your requirements.

Static reports
Ready-to-use reports that are bundled with the Security Identity Manager reporting packages.

IBM Cognos reporting framework overview

IBM Security Identity Manager Cognos reporting framework customizes the IBM Security Identity Manager reports to your specifications.

This document provides the following information about the IBM Security Identity Manager Cognos report model:

- Prerequisite installation and configuration tasks for the report models.
- Detailed description of the `Recertification`, `Accounts`, `Provisioning`, `Roles`, `Separation of duty`, `Users`, `Services`, and `Access` models. The descriptions include the namespaces, query subjects, and query items.
- Types of static reports that are created with the report model.
- References for mapping the attributes and entities, the common tasks for configuring any IBM Cognos report model, or scenario that describes how to customize the report.

IBM Cognos reporting components

The topic describes IBM Cognos 10.2.1 Fix Pack 1 reporting components that you might use while you work with IBM Security Identity Manager Cognos report models.

Query Studio

Query Studio is the reporting tool for creating simple queries and reports in IBM Cognos Business Intelligence. To use Query Studio effectively, you must be familiar with your organization's business and its data. You might also want to be familiar with other components of IBM Cognos Business Intelligence.

Report Studio

Report Studio is a Web-based report authoring tool that professional report authors and developers use to build sophisticated, multiple-page, multiple-query reports against multiple databases. With Report Studio, you can create any reports that your organization requires, such as invoices, statements, and weekly sales and inventory reports.

Your reports can contain any number of report objects, such as charts, crosstabs, lists, and also non-BI components such as images, logos, and live embedded applications that you can link to other information.

IBM Cognos Connection

IBM Cognos Connection is the portal to IBM Cognos software. IBM Cognos Connection provides a single access point to all corporate data available in IBM Cognos software.

You can use IBM Cognos Connection to create and run reports and cubes and distribute reports. You can also use it to create and run agents and schedule entries.

Framework Manager

Framework Manager is a metadata modeling tool that drives query generation for IBM Cognos software. A model is a collection of metadata that includes physical information and business information for one or more data sources.

IBM Cognos software enables Performance Management on normalized and denormalized relational data sources and various OLAP data sources. When you add security and multilingual capabilities, one model can serve the reporting, ad hoc querying, and analysis needs of many groups of users around the globe.

Before you do anything in IBM Cognos Framework Manager, you must thoroughly understand the reporting problem that you want to solve.

Prerequisites for IBM Cognos report server

Security Identity Manager supports IBM Cognos Business Intelligence Server version 10.2.1 Fix Pack 1.

You must install the software in the following table to work with IBM Security Identity Manager Cognos reports.

Table 15. Software requirements for IBM Cognos report server

Software	For more information, see
IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for **Business Intelligence Installation and Configuration Guide 10.2.1**. 3. Search for the installation information and follow the procedure.
Web server	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. In the right pane of the home page, under **Supported hardware and software** section, click **IBM Cognos 10.2.1 Business Intelligence software environments**. 3. Click **10.2.1** tab. 4. Click **Software** in the **Requirements by type** column under the section **IBM Cognos Business Intelligence 10.2.1**. 5. Search for **Web Servers** section.
Data sources	1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. In the right pane of the home page, under **Supported hardware and software** section, click **IBM Cognos 10.2.1 Business Intelligence software environments**. 3. Click **10.2.1** tab. 4. Click **Software** in the **Requirements by type** column under the section **IBM Cognos Business Intelligence 10.2.1**. 5. Search for **Data Sources** section.

Note: Optionally, you can install IBM Framework Manager, version 10.2.1 Fix Pack 1 if you want to customize the reports or models.

Note:

Security Identity Manager version 6.0.0.6 supports IBM Cognos Business Intelligence Server, version 10.2.1 as well as version 10.2.2. By default, the Security Identity Manager version 6.0.0.6 report package is packaged with IBM Cognos Business Intelligence Server, version 10.2.1.

Reports in the IBM Cognos Business Intelligence Server, version 10.2.1 can run in the IBM Cognos Business Intelligence Server, version 10.2.2. However, if you work with IBM Cognos Business Intelligence Server, version 10.2.2, the compatibility with an earlier versions of IBM Cognos Business Intelligence Server is not supported. For more information about installation and configuration of IBM Cognos Business Intelligence Server, version 10.2.2, see http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.2/com.ibm.swg.ba.cognos.cbi.doc/welcome.html?.

Installation of IBM Cognos reporting components

Installation of IBM Cognos reporting components is optional. You need these components only if you use the Cognos based reports. You must complete the installation and data synchronization process before you can access and work with IBM Security Identity Manager Cognos reports.

Note: IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use DB2 database or Oracle database instead.

The following table describes the installation and synchronization process.

Table 16. Installation and data synchronization process

Task	For more information
Install Cognos Business Intelligence.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Install Cognos BI on one computer**.
Install Framework Manager.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Installing Framework Manager**.
Complete the data synchronization.	See “Data synchronization” on page 336. **Note:** Run the data synchronization before you generate the reports to obtain the latest report data.

Cognos reporting

Security Identity Manager Version 6.0 fix pack 6 installs Cognos reports and models. To use these new reports and models, see the Cognos reporting documentation at IBM Cognos Business Intelligence documentation.

You can find the Cognos reports and models that are specific to Security Identity Manager at:

- `<isim_home>/extensions/6.0/Cognos/Model/ISIMReportingModel_6.0.0.6.zip`
- `<isim_home>/extensions/6.0/Cognos/Reports/ISIMReportingPackage_6.0.0.6.zip`

Note: You must set the locale to English or to any supported language before you run any of the reports. See “Setting language preferences” on page 205. Otherwise, you might encounter a "Language not supported" issue.

Configuration of IBM Cognos reporting components

After you install the prerequisites for the IBM Security Identity Manager Cognos Business Intelligence server, configure the Framework Manager, and create a content store database. Then, configure the web gateway and web server.

During the database configuration process, ensure that you complete the points in the following note.

Note:

- IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use DB2 database or Oracle database instead.
- Set the `JAVA_HOME` environment variable to point to the JVM used by the application server.
- You must use the enterprise database as IBM Cognos content store.
- Delete the existing data source and create a new data source to enable an option of generating DDL during creation of the content store database. For information about data source creation, see “Creating a data source” on page 196.

The following table describes the configuration process.

Each step requires that you search in the Knowledge Center for IBM Cognos Business Intelligence, which is at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html

Table 17. Configure IBM Cognos reporting components

Task	For more information
Configure Framework Manager.	Search for **Configuring Framework Manager on a 64-bit computer**.
Create a content store in the database.	Search for **Start IBM Cognos Configuration**, complete the steps as per your operating system, then search for **Create a content store database**.
Configure the web gateway.	Search for **Configure the gateway**.
Configure your web server.	Search for **Configure your web server**..

Setting report server execution mode

You must have a report server execution mode that is set to 32-bit mode for the report packages that do not use dynamic query mode.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** panel, click **Environment**.
3. Click the **Value** box for **Report server execution mode**.
4. Select **32-bit**.
5. From the **File** menu, click **Save**.

What to do next

Restart the IBM Cognos service. Complete the following steps:

1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Restarting the IBM Cognos service to apply configuration settings**.

Setting environment variables

You must set the database environment variables for a user before you start the IBM Cognos processes.

Procedure

1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Database environment variables**.

What to do next

Start the Cognos service from IBM Cognos Configuration to host the IBM Cognos portal. Complete the following steps:

1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Starting or stopping the Cognos service**.

Editing the ISIM Environment dashboard refresh interval

You can edit the refresh interval for your software deployment depending on the requirements of your organization.

Procedure

1. Open the ISIM Environment Dashboard in the Report Studio.
2. Navigate to the Page explore tab in the Report Studio.
3. Open the ISIM Environment Dashboard page.
4. Look for the `<HTML Item>` highlighted on the page.
5. Double click to edit the page. Specify the interval in seconds and save the report.

What to do next

You must do the similar task for the dashboard sub report which contains more dashboard details.

Note: All the sub reports are hidden by default. To view all the hidden reports:

1. Open the Cognos connection portal.
2. Select **My Area** > **My Preferences**.
3. Select **Show hidden** entries.

Importing the report package

Import the report package to work with the bundled report models and the static reports.

Before you begin

- Copy the `ISIMReportingPackage_6.0.0.6.zip` file to the directory where your deployment archives are saved. The default location is `10_location/deployment`. For more information about the reporting packages, see "Installation of IBM Cognos reporting components" on page 193.
- To access the **Content Administration** area in IBM Cognos Administration, you must have the required permissions for the administration tasks secured feature.

Procedure

1. Access the IBM Cognos Gateway URI. For example, `https://`*`hostname:port`*`/ibmcognos/cgi-bin/cognos.cgi`. The *localhost* is the IP address or network host name where IBM Cognos gateway is configured. The *portnumber* is the port on which the IBM Cognos gateway is configured.
2. Go to **Launch**.
3. In the IBM Cognos Administration window, click the **Configuration** tab.
4. Click **Content Administration**.
5. Clear the history.
6. On the toolbar, click `New Import` icon. The New Import wizard opens.
7. In the **Deployment Archive** box, select **ISIMReportingPackage_6.0.0.6**.
8. Click **Next**.
9. In the **Specify a name and description** window, you can add the description and screen tip.
10. Click **Next**.
11. In the **Select the public folders and directory content** window, select the model that is displayed.
12. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and an owner for the entries after they are imported.
13. Click **Next**. The summary information opens.
14. Review the summary information. Click **Next**.
15. In the **Select an action** page, click **Save and run once**.
16. Click **Finish**.
17. Specify the time and date for the run.
18. Click **Run**.
19. Review the run time. Click **OK**.
20. When the import file operation is submitted, click **Finish**.

Results

You can now use the report package to create reports and to run the sample reports. The sample reports are available in the reporting model on the **Public Folders** tab in the IBM Cognos portal.

Creating a data source

To work with the IBM Security Identity Manager Cognos reports, you must create a data source.

Before you begin

- You must use the data source name as `ISIM`.

- If you are working with DB2 database client, copy the file `db2cli.dll` from the DB2 client installation directory to the *<IBM Cognos installation directory>*`/bin` folder.
- The data source must be pointed to the IBM Security Identity Manager enterprise database. For example, IBM DB2. After the data synchronization, the data is in the IBM Security Identity Manager enterprise database.

Procedure

1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Creating a data source** and complete the steps.

What to do next

Note: Corrupted attribute names are displayed in the reports for `Arabic`, `Chinese`, `Hebrew`, `Japanese`, `Korean`, and `Russian` languages. Double-byte character set (DBCS) characters appear to be corrupted in the reports. Edit the data source so that the data flow is in Unicode format. Complete the following steps:

1. On the Work with Reports page, click **Launch** > **IBM Cognos Administration**.
2. Click **Configuration** to open the data source connection.
3. Click **ISIM**.
4. Under the **Actions** column, click **Set properties-ISIM**.
5. On the **Set properties-ISIM** window, click **Connection**.
6. In the **Connection String** field, click the pencil symbol to edit the connection string.
7. In the **Collation Sequence** field, type `@UNICODE`.
8. Click **OK**.
9. Run the report to verify that the text is no longer corrupted.

Enabling the drill-through for PDF format

You must enable the drill-through functionality to run the drill-through reports in the PDF format.

Before you begin

Disable any pop-up blocking software in the browser.

Procedure

1. Open IBM Cognos Configuration.
2. Specify the fully qualified domain name for all the URIs that are defined.
3. Save the configuration.
4. Restart the IBM Cognos service. Complete the following steps:
   a. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
   b. Search for **Restarting the IBM Cognos service to apply configuration settings**.
5. In the **Explorer** window, click **Environment**.
6. In the **Group Properties** window, copy the value in the **Gateway URI** box.

7. Paste the copied **Gateway URI** value in the supported browser.
8. Run the report that you want.

Results

The drill-through report is run successfully in the PDF format.

Security layer configuration around the data model and reports

An access to the data model and reports can be restricted to a set of authorization roles. The users can create the authorization roles and associate them with the reporting entities. Only entitled users can access the data model or reports.

Authentication and authorization for IBM Cognos reports

IBM Cognos Business Intelligence administrators can set up the folders that store the reports. They can then secure those folders so that only authorized users can view, change, or perform other tasks by using the reports in the folder. To set up access control on the reports, administrators can set up the user authentication and define the access control for the set of users.

User authentication setup by using LDAP

You can configure IBM Cognos 10.2.1 Fix Pack 1 components to use an LDAP namespace for authentication when the users are in an LDAP user directory.

Configuring an LDAP Namespace for IBM Directory Server:

If you configure a new LDAP namespace for use with the IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.

Procedure

1. Open IBM Cognos Configuration.
2. In the Explorer window, under **Security**, right-click **Authentication**.
3. Click **New resource** > **Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click **LDAP-General default values**.
6. Click **OK**. The new authentication namespace resource appears in the Explorer window, under the **Authentication** component.
7. In the Properties window, for the **Namespace ID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
   For **Host and Port**, specify `<Hostname>:<port>`. For example, `localhost:389`.
8. Specify the values for all other properties to ensure that IBM Cognos 10.2.1 Fix Pack 1 can locate and use your existing authentication namespace.
   - For **Base Distinguished Name**, specify the entry for a user search.
   - For **User lookup**, specify `(uid=${userID})`.
   - For **Bind user DN and password**, specify `cn=root`. For example, `cn=root` as a user name and `secret` as a password.

Note: Specify the values if you want an LDAP authentication provider to bind to the directory server by using a specific bind user DN and password. If no values are specified, an LDAP authentication namespace binds as anonymous.

9. If you do not use external identity mapping, use bind credentials to search an LDAP directory server. Complete the following items.
   - Set **Use external identity** to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.
10. To configure an LDAP advanced mapping properties, see the values that are specified in the following table.

Table 18. LDAP advanced mapping values

Mappings	LDAP property	LDAP value
Folder	Object class	`organizationalunit`, `organization`, and `container`
	Description	`description`
	Name	`ou`, `o`, and `cn`
Group	Object class	`groupofnames`
	Description	`description`
	Member	`member`
	Name	`cn`
Account	Object class	`inetorgperson`
	Business phone	`telephonenumber`
	Content locale	`(leave blank)`
	Description	`description`
	Email	`mail`
	Fax/Phone	`facsimiletelephonenumber`
	Given name	`givenname`
	Home phone	`homephone`
	Mobile phone	`mobile`
	Name	`cn`
	Pager phone	`pager`
	Password	`userPassword`
	Postal address	`postaladdress`
	Product locale	`(leave blank)`
	Surname	`sn`
	Username	`uid`

If the schema is modified, you must make extra mapping changes.

11. To prevent the anonymous access, complete the following steps:
    a. Go to **Security** > **Authentication** > **Cognos**.
    b. Set **Allow anonymous access?** to **False**.
12. From the **File** menu, click **Save**.

Results

A new LDAP namespace is configured with the appropriate values.

What to do next

Create the users in an LDAP. See "Creating users in an LDAP."

Creating users in an LDAP

See the example in this procedure that uses an LDAP utility to create users in LDAP.

Procedure

1. Open an LDAP utility. For example, if you are using the IBM Directory Server, the LDAP utility is `idsldapadd`.
2. Import the sample file `LdapEntries.ldif` that lists all the users who are authorized to access the reports. See the following example.

Results

After the successful import operation, you can see the users that are created in `ou=users,ou=SWG`.

Example

A sample file: `LdapEntries.ldif`

In this example, `dc=com` is the root entry. Specify the entry according to the schema that you use.

```
dn: ou=SWG, dc=com
ou: SWG
objectClass: top
objectClass: organizationalUnit

dn: ou=users,ou=SWG, dc=com
ou: users
objectClass: top
objectClass: organizationalUnit

dn: uid=steves,ou=users,ou=SWG, dc=com
uid: steves
userPassword:: hello123
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Wiley
cn: Steves

dn: uid=PortalAdmin,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: PortalAdmin
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Poon
cn: Chuck

dn: uid=william,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: william
objectClass: inetOrgPerson
objectClass: top
objectClass: person
```

```
objectClass: organizationalPerson
sn: Hanes
cn: William

dn: uid=lucy,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: lucy
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Haye
cn: Lucy
```

What to do next

Authenticate IBM Cognos by using an LDAP user. Complete these steps:

1. Access the IBM Cognos Gateway URI. For example, `http://localhost:portnumber/ibmcognos/cgi-bin/cognos.cgi`. The *localhost* is the IP address or network host name where IBM Cognos gateway is configured. The *portnumber* is the port on which the IBM Cognos gateway is configured.
2. Select the configured **Namespace**, and click **OK**.
3. Enter your LDAP user ID and password.
4. Click **OK**.

Access control definition for the reports and reporting packages

You can define the access control for the LDAP users who are the members of a role that is defined in the IBM Cognos namespace. Access can be granted to those users who are the members of a defined role.

A user who has the system administrator privileges can grant the access.

Initially, all users are the members of the system administrator. Therefore, you can log in with your LDAP user authentication in IBM Cognos and access the administration section before you restrict the administration access.

Restricting administration access and adding an LDAP user to system administrator role:

You can restrict the IBM Cognos administration access by using the system administrators role in IBM Cognos namespace. You can also add an LDAP user to the system administrator role for IBM Cognos report administration.

Procedure

1. Log in to IBM Cognos with an LDAP user whom you want to assign the system administrator role.
2. Go to **Launch**, and click **IBM Cognos Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Navigate to **System Administrator** role.
6. Click the **More** link.
7. Under **Available actions**, click **Set properties**.
8. Click the **Members** tab.
9. Click the **Add** link.
10. Under **Available entries** section, click an LDAP namespace.

11. Select the **Show users in the list** check box.
12. Select the user whom you want to assign the system administrator role and make it into selected entries list.
13. Click **OK**.
14. Select **Everyone** from the members entry.
15. Click the **Remove** link to ensure that only the added users can have the system administration access.
16. Click **OK**.
17. Click the **Permissions** tab.
18. Verify that the system administrators are listed and they are provided all the permissions.

    If no permissions are provided, then select the system administrators and grant all the permissions. Select the **Override the access permissions acquired from the parent entry** check box to grant the permissions.
19. Click **OK**.

Results

An LDAP user is added with the system administrator role.

What to do next

Create a role and add LDAP users as the members to that role. See "Creating a role and adding LDAP users as members."

Creating a role and adding LDAP users as members:

The topic describes the procedure to create a role in IBM Cognos and add the members from an LDAP namespace to it.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Go to **Launch**, and click **IBM Cognos Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Click the **New Role** icon from the palette.
6. Specify the name for a role. For example, `ISIMAuditor`.
7. Add the description and the screen tip.
8. Click **Next**.
9. Under **Select the members**, click **Add**.
10. Under **Available Entries Directory**, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the users whom you want to add as the members to the role and make it into selected entries list.
13. Click **OK**.
14. Click **Finish**.

Results

A new role is created and LDAP users are added as the members to the new role.

Defining an access to the report by using a role:

You can define an access to the report by using a role. All the members of a role can access the report or reports.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Under **Public Folders**, click the `ISIMReportingPackage_6.0.0.4.zip`.
3. Click the **More** link on the **Actions** toolbar that is associated with the report for which you want to provide the access.
4. Under **Available actions**, click **Set properties**.
5. Click the **Permissions** tab.
6. Select the **Override the access permissions acquired from the parent entry** check box.
7. Click **Add** link at the bottom of the list of entries.
8. Click **Cognos**.
9. Select the role that you want to add and make it to the selected entries.
10. Click **OK**.
11. Select the role and grant the permissions.
12. Optional: Remove other roles for which you do not want to provide the access.
13. Click **OK**.

Results

An access is defined to the report by using a role and all the members of a role can access the reports.

Defining an access to the reporting package by using a role:

You can define an access to the report package by using a role. All the members of a role can access the report package.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Under **Public Folders**, click the **More** link on the **Actions** toolbar that is associated with the `ISIMReportingPackage_6.0.0.4.zip`.
3. Under **Available actions**, click **Set properties**.
4. Click the **Permissions** tab.
5. Select the **Override the access permissions acquired from the parent entry** check box.
6. Click the **Add** link at the bottom of the list of entries.
7. Click **Cognos**.
8. Select the role that you want to add and make it to the selected entries.
9. Click **OK**.

10. Select the role and grant the permissions.
11. Optional: Remove other roles for which you do not want to provide the access.
12. Click **OK**.

Results

An access is defined for the reporting package by using a role and the members of a role can access the reporting package.

References for IBM Cognos report security configuration

Use the following references that provide information about the topics that are related to the security configuration for the IBM Cognos reports.

Access the IBM Cognos Business Intelligence 10.2.1 documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html and search for the following terms.

- **Security model**.
- **Authentication providers**.
- **Add or remove members of a cognos group or role**.
- **Create a cognos group or role**.
- **Authorization**.
- **Access permissions and credentials**.

Globalization overview

You can use the globalization features of IBM Security Identity Manager Cognos report models to produce the reports in your own language.

Language support overview

IBM Security Identity Manager Cognos reports support the following languages.

- cs=Czech
- de=German
- en=English
- es=Spanish
- fr=French
- hu=Hungarian
- it=Italian
- ja=Japanese
- ko=Korean
- pl=Polish
- pt_BR=Brazilian Portuguese
- ru=Russian
- zh_CN=Simplified Chinese
- zh_TW=Traditional Chinese
- nl=Dutch
- tr=Turkish
- el=Greek - partially supported.

Note:

The IBM Cognos Business Intelligence Server 10.2.1 Fix Pack 1 is not fully translated into the Greek language. Only components like `Cognos Viewer`, `Cognos Connection`, `Cognos Administration`, and `Cognos Workspace` support translation in Greek language.

Messages or terms related to the globalization

In the reports, some of the column values might display the term `Language not supported`

When you select the language that is not supported by the reporting model, the value in the column is displayed as `Language not supported`.

Setting language preferences

You can personalize the way data appears in IBM Cognos workspace by changing your preferences. You can set the product language or content language to get the preferred output format of the reports.

Before you begin

Install and configure the IBM Cognos Business Intelligence Server.

Procedure

1. In the IBM Cognos Connection window, click **My Area Options** menu button.
2. Click **My Preferences**.
3. In the Set Preferences window, under the **Regional options** section, select **Product language**. Product language specifies the language that the IBM Cognos user interface uses.
4. In the Set Preferences window, under the **Regional options** section, select **Content language**. Content language specifies the language that is used to view and produce content in IBM Cognos such as data in the reports.
5. Click **OK**.

Results

You can view the reports or user interface in the language that you specified.

Report models

Use the following information about the objects and the report model names, namespaces, and entities to work with the report models.

Report model objects and their definitions

Use these definitions to work with IBM Security Identity Manager Cognos report models.

Query Items

The smallest piece of the model in a report. It represents a single characteristic of something, such as the date that a product was introduced.

Query subjects or dimensions contain query items. For example, a query subject that references an entire table contains query items that represent each column in the table.

Query items are the most important objects for creating reports. They use query item properties of query items to build their reports.

Query Subjects
A set of query items that have an inherent relationship. In most cases, query subjects behave like tables. Query subjects produce the same set of rows regardless of which columns were queried.

Packages
A subset of the dimensions, query subjects, and other objects that are defined in the project. A package is published to the IBM Cognos server. It creates reports, analyses, and ad hoc queries.

Namespaces
Uniquely identifies query items, dimensions, query subjects, and other objects. You import different databases into separate namespaces to avoid duplicate names.

Recertification model

You can use the recertification model to customize the reports that are related to the recertification audit and configuration.

The recertification model for IBM Security Identity Manager consists of these namespaces:

Table 19. Recertification model namespaces

Namespace	For information about query subjects and query items, see
`Recertification Audit`	"`Recertification Audit` namespace" on page 218.
`Recertification Config`	"`Recertification Config` namespace" on page 228.

Accounts model

You can use the accounts model to customize the account audit and configuration reports.

The accounts model for IBM Security Identity Manager consists of two namespaces:

Table 20. Accounts model namespaces

Namespace	For information about query subjects and query items, see
`Account Audit`	"`Account Audit` namespace" on page 234.
`Account Configuration`	"`Account Configuration` namespace" on page 239.

Provisioning model

You can use the provisioning model to customize the provisioning policy audit and configuration reports.

The provisioning model for IBM Security Identity Manager consists of two namespaces:

Table 21. Provisioning model namespaces

Namespace	For information about query subjects and query items, see
`Provisioning Policy Audit`	"`Provisioning Policy Audit` namespace" on page 248.
`Provisioning Policy Config`	"`Provisioning Policy Config` namespace" on page 251.

Roles model

You can use the roles model to create the role audit and configuration reports.

The roles model for IBM Security Identity Manager consists of two namespaces:

Table 22. Roles model namespaces

Namespace	For information about query subjects and query items, see
`Role Audit`	"`Role Audit` namespace" on page 255.
`Role Configuration`	"`Role Configuration` namespace" on page 258.

Note: If you want to run a Role and Policy Modeler report for the roles with IBM Security Identity Manager data, you must rewrite the report or use an existing predefined report in the IBM Security Identity Manager 6.0 Cognos package.

Separation of duty model

You can use the separation of duty model to customize the separation of duty policy audit and configuration reports.

The separation of duty model for IBM Security Identity Manager consists of two namespaces:

Table 23. Separation of duty model namespaces

Namespace	For information about query subjects and query items, see
`Separation of Duty Audit`	"`Separation of Duty Audit` namespace" on page 265.
`Separation of Duty Configuration`	"`Separation of Duty Configuration` namespace" on page 271.

Users model

You can customize the user configuration reports with the users model.

The users model for IBM Security Identity Manager consists of the `User Configuration` namespace. For information about query subjects and query items, see "`User Configuration` namespace" on page 273.

Services model

You can customize the audit reports with the services model.

The services model for IBM Security Identity Manager consists of the `Service Audit` namespace. For information about query subjects and query items, see "`Service Audit` namespace" on page 281.

Access model

You can customize the audit and configuration reports with the access model.

The access model for IBM Security Identity Manager consists of these namespaces:

Note: The new `Access Audit` model is developed for Identity Service Center. An old `Access Audit` model is renamed to `Access Audit(Deprecated)`.

Table 24. Access model namespaces

Namespace	For information about query subjects and query items, see
`Access Audit(Deprecated)`	"`Access Audit(Deprecated)` namespace" on page 284.
`Access Configuration`	"`Access Configuration` namespace" on page 293.
`Access Audit`	"`Access Audit` namespace" on page 289.

Report descriptions and parameters

The topics provides information about the IBM Security Identity Manager Cognos static reports that are bundled with the package. You can view the list of reports and the namespaces used to create these reports. Use the parameters and their descriptions information while you generate the reports.

Note:

- You must map the attributes to the entities before you work with the following reports. For more information about mapping the attributes, see "Mapping the attributes and entities" on page 299.
- You must set the locale to English or to any supported language before you run any of the reports. See "Setting language preferences" on page 205. Otherwise, you might encounter a "Language not supported" issue.
- Use the percent symbol (%) as a default search character in all the reports.
- Any time stamp in the following reports is in Greenwich Mean Time (GMT) format.
- Use the Report Studio to change the column title names in the layout to meet the specific needs of your company.

You can choose the output format of the reports. For more information about the supported report format, complete the following steps.

1. Access the IBM Cognos Business Intelligence documentation at http://www-01.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Report Formats**.

Note: You can export the report data in plain format if you use formats other than HTML or PDF. The reports that are generated in such formats do not support some of the IBM Cognos interactive features. For example, `charts`.

Use HTML or PDF formats for running interactive reports.

The following table lists the reports and the namespaces that generate them.

Table 25. Reports and the namespaces

Reports	Namespace used
Access Definition Report	• `Access Audit` • `Access Configuration`
Account Status Report	`Account Audit`
Audit History Report	`Access Audit` and `Account Audit`
Entitlements Report	`Provisioning Policy Configuration`

Table 25. Reports and the namespaces (continued)

Reports	Namespace used
IBM Security Identity Manager Dashboard	Account Configuration, Provisioning Policy Configuration, User Configuration, and Service Audit (Entity Name Service)
Recertification Definition Report	Recertification Config
Separation of Duty Policy Definition Report	Separation of Duty Configuration
Separation of Duty Policy Violation Report	Separation of Duty Audit
Services Report	Service Audit
User Access Report	Access Configuration
User Recertification History Report	Recertification Audit

Note: The access that is defined on groups and roles cannot be displayed in the User Access Report if the access is disabled.

The following table lists the subreports. These reports are the operational reports and the subsets of the main reports. The subreports are hidden and started from the main reports.

Table 26. Subreports

Main report	Subreports
Entitlements Report	• Entitlements Sub Report • Entitlements Sub_Sub Report
IBM Security Identity Manager Dashboard	Dashboard sub reports
Recertification Definition Report	• Access Recertification Definition Sub Report • Account Recertification Definition Sub Report • User Recertification Definition Sub Report
Separation of Duty Policy Definition Report	Separation of Duty Policy Definition Sub Report
Separation of Duty Policy Violation Report	Separation of Duty Violation Definition Sub Report
User Recertification History Report	User Recertification History Sub Report

Access Definition Report

The report provides information about the access definitions. Use the report to view the accesses that are configured in an organization.

After you select the parameter values, the Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 27. Filters for access definition report

Parameter	Description
Access	Displays the list of accesses for which you want to generate a report.

Table 27. Filters for access definition report (continued)

Parameter	Description
Access Search Terms	Displays the list of search terms that are defined for an access.
Access Badge Text	Displays the description about the badge that is defined for an access.
Access Type	Displays the type of an access. The type of an access can be a role, application, shared folder, email group, or custom access that is defined in an organization.

You must define the base icon URL path in the query of the access definition report to display the icons in the report. For more information, see "Defining the base icon URL path" on page 217.

Account Status Report

The report shows the status of an account such as compliant, disallowed, orphan, non-compliant, and suspend. Use the report to view the status of accounts that are provisioned on the different managed resources.

After you select the parameter values, the Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 28. Filters for Account Status Report

Parameter	Description
Service	Displays the list of all the services that have one or more accounts provisioned.
Account Status	Displays the status and states of the accounts that are created in an organization. The states of an account are compliant, disallowed, orphan, non-compliant, and suspend.

Audit History Report

The Audit History Report provides information about the history of audits. You can generate the audit history reports for access, account, and a user.

You can generate the following types of subreports from the audit history report.

Note: Use the account audit model and reports to view the details about the accounts that are associated with a user. Use the access audit model and reports to view the details about the accesses that are associated with a user. If the account is on the service that is defined as an access, the audit details can be seen only in the `Access Audit` report.

Table 29. Audit History subreports

Subreport name	In the Audit Report Type drop-down list
Access audit report.	Select **Access**. For more information about the access audit report parameters and their descriptions, see "Access audit history report" on page 211.

Table 29. Audit History subreports (continued)

Subreport name	In the Audit Report Type drop-down list
Account audit report.	Select **Account**. For more information about the account audit report parameters and their descriptions, see "Account audit history report."

After you select the values for the parameters, the Prompt Page Summary is generated. The Prompt Page Summary provides information about the selected parameters and their values in a table.

Access audit history report:

Use this report to view the history of actions that are performed on an access in Identity Service Center.

After you select the values for the following parameters, the Prompt Page Summary is generated. The Prompt Page Summary provides information about the selected parameters and their values in a table.

Note:

- If the account is on the service that is defined as an access, the audit details can be seen only in the `Access Audit` history report.
- The parameter filter values are displayed if the access is requested through Identity Service Center.

The following table describes the parameters for filtering the report.

Table 30. Filters for access audit history report

Parameter	Description
`Audit Report Type`	Lists the audit type of reports. Select `Access` from the list.
`Audit Start Date`	Displays all audited actions and operations on an access approved from the specified date.
`Audit End Date`	Displays all audited actions and operations on an access approved until the specified date.
`Access Business Unit`	Displays the business unit that is associated with an access.
`Access Name`	Lists the names of all accesses that are available.
`Requestee Name`	Displays the name for whom the access is requested.
`Audit Action`	Displays an action that is performed on an access. The supported audit actions are `Add Member` and `Remove Member`.
`Approver`	Displays the name of a user who approves the audit.
`Approval Status`	Displays the status of the approval. The supported approval statuses are `Approved`, `Rejected`, and `Pending`.

Account audit history report:

Use this report to view the history of actions that are performed on an account.

After you select the values for the following parameters, the Prompt Page Summary is generated. The Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 31. Filters for account audit history report

Parameter	Description
Audit Report Type	Lists the audit type of reports. Select `Account` from the list.
Audit Start Date	Displays all audited actions and operations on accounts approved from the specified date.
Audit End Date	Displays all audited actions and operations on accounts approved until the specified date.
Account Business Unit	Displays the business unit that is associated with an account.
Account Service Name	Displays the list of all the services that have one or more accounts provisioned.
Account Name	Displays the list of all the accounts that are created in an organization. If you want to generate an account audit report for all the accounts that are deleted, then do not provide any filter parameter.
Account Owner	Displays the user who owns one or more accounts in an organization.
Audit Action	Displays an action that is performed on a person or the business partner person. The supported audit actions are `Add`, `Adopt`, `Delete`, `Orphan`, `Restore`, `Suspend`, `Synchronize Password`, and `Change Password`.
Approver	Displays the name of a user who approves the audit.
Approval Status	Displays the status of the approval.

Entitlements Report

Use the report to view the list of services to which an individual is entitled. The report also lists all users and their entitlements.

After you select the parameter values, the Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 32. Filters for Entitlements Report

Parameter	Description
Provisioning Policy	Displays the list of provisioning policies.
Entitlement	Displays the list of services to which a user is entitled.

After you generate the report, the provisioning policy definition lists the entitlements and configuration information about the members who are entitled to the provisioning policy.

All Users
: All users in the organization who are entitled to the provisioning policy.

Roles The roles whose members are entitled to the provisioning policy.

All Other Users
: All other users who are not granted to the entitlements that are defined by this provisioning policy by way of other policies.

To drill-through information about the users and their entitlements, complete the following steps:

1. Click the link in the **Member** column to list all the members who are entitled to a service.
2. Click the link in the **User First Name** column to list all the entitlements that are granted for a specified user.

IBM Security Identity Manager Dashboard

A dashboard is a group of objects, such as charts, indicators, or tables. View the dashboard to access the detailed information about IBM Security Identity Manager environment.

The dashboard provides a quick summary about the IBM Security Identity Manager environment to an administrator or business user.

The dashboard shows information about the key activities and size metrics. It is more intended as the business side of an environment. For example, you can get a glance of how large is the IBM Security Identity Manager environment in your company.

The dashboard provides information about the following entities. You can specify the scope of the information that is displayed in the dashboard by using the available filters in some of the view types.

The dashboard requires that you map the attributes and entities of the following namespaces:

- Account Configuration
- Provisioning Policy Configuration
- User Configuration
- Service Audit (Entity Name Service)

See "Mapping the attributes and entities" on page 299 for the details.

Environment Overview
: This view shows the statistical chart of registered accounts, provisioning policies, resources, roles, separation of duty policy violations and users in the IBM Security Identity Manager environment. Information is presented in a block diagram.

Entity View
: This view shows the statistical diagram and chart of managed users, managed resources, managed roles, and provisioning policy memberships for the selected business units. You select the business units that you want to view in the dashboard.

Account Status View
: This view shows the statistical chart of non-compliant accounts, orphan accounts, suspended accounts, and disallowed accounts for the selected services. You select the services that you want to view in the dashboard.

Separation Of Duty Policy Violations
: This view shows the statistical chart of violations in the organization for each Separation Of Duty policy.

Recertification Definition Report

Use the report to view the recertification policies and their schedule. These recertification policies are filtered by the recertification target type, policy name, and business unit.

You can generate the following types of subreports from the recertification definition report.

Table 33. Recertification Definition subreports

Subreport name	In the Recertification Target Type drop-down list
Access recertification definition report	Select **Access**.
Account recertification definition report	Select **Account**.
User recertification definition report	Select **User**.

After you select the values for the following parameters, the Prompt Page Summary is generated. The Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 34. Filters for Recertification Definition Report

Parameter	Description
Recertification Policy Business Unit	Displays the business unit.
Recertification Policy Name	Displays the name of the recertification policy.
Recertification Target Type	Displays the type of the recertification. The possible values are `Access`, `Account`, and `User`.

In the Content page, you can view the recertification policies that are filtered by the recertification target type, policy name, and business unit that you selected. You can view the configuration details by clicking the recertification policy name.

Separation of Duty Policy Definition Report

Use the report to list the separation of duty policies that are filtered by the policy name and business unit. The report provides information about the owners, rules, and roles that are associated with a separation of duty policy. An owner can be a person, role, or both.

After you select the parameter values, the Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 35. Filters for Separation of Duty Policy Definition Report

Parameter	Description
Separation of Duty Policy	Lists the names of the available separation of duty policies.
Business Unit	Lists the names of the available business units.

After you generate the report, the report page shows the separation of duty policy, business unit, and whether the policy is enabled or not.

Click the policy name to obtain details such as owners, rules, and roles that are associated with a separation of duty policy. An owner can be a person, role, or both.

Separation of Duty Policy Violation Report

This report contains the person, policy, and rules violated, approval, justification (if any), and who requested the violating change.

After you select the values for these parameters, the Prompt Page Summary is generated. The Prompt Page Summary provides information in tabular format about the selected parameters and their values.

The following table describes the parameters for filtering the report.

Table 36. Filters for Separation of Duty Policy Violation Report

Parameter	Description
Separation of Duty Policy Business Unit	Displays the name of the business unit.
Separation of Duty Policy	Displays name of the separation of duty policy.
Separation of Duty Policy Rule Description	Displays the description of the rule name that is associated with the separation of duty policy.

Services Report

The report lists the services that are defined in IBM Security Identity Manager. The report can be filtered by the service business unit, service, and service owner.

After you select the parameter values, the Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 37. Filters for Services Report

Parameter	Description
Service Business Unit	Lists the business units of the services.
Service	Displays the list of all the services that are defined in the IBM Security Identity Manager.
Service Owner	Lists the owners of the services.

User Access Report

The User Access Report provides information about the different users in a business unit and their access. The user is entitled to at least one access.

You can generate the following types of subreports from the User Access Report.

Table 38. User Access subreports

Subreport name	In the Report Type list
User Access Report - View by Access	Select **View by Access**. For more information about the report parameters and their descriptions, see “View by Access” on page 216.

Table 38. User Access subreports (continued)

Subreport name	In the Report Type list
User Access Report - View by User	Select **View by User**. For more information about the report parameters and their descriptions, see "View by User."

You must define the base icon URL path in the query of the User Access Report to display the icons in the report. For more information, see "Defining the base icon URL path" on page 217.

View by Access:

With this report type, the User Access Report focuses on the list of all access. You have the option to view the corresponding user for the selected access.

The following table describes the parameters for filtering the report.

Table 39. Filters for the User Access report - View by Access report type

Parameter	Description
Access Name	Displays the list of accesses for which you want to generate a report.
Access Search Terms	Displays the list of search terms that are defined for an access.
Access Badge Text	Displays the description about the badge that is defined for an access.
Access Type	Displays the type of an access. The type of an access can be a role, an application, a shared folder, an email group, or a custom access that is defined in an organization.

Select the values for these parameters, then click **Finish** to generate the report.

The Prompt Page Summary provides an overview of the report parameters and the selected values. The next page lists all of the access that you filtered, with their details.

Click the *Access Name* link to view the corresponding user of the selected access. Information about the user such as user type and business unit is provided.

View by User:

With this report type, the User Access Report focuses on the list of users per business unit. You have the option to view all access corresponding to each of these users.

The following table describes the parameters for filtering the report.

Table 40. Filters for the User Access report - View by User report type

Parameter	Description
User Business Unit	Displays the list of user business units, for which you want to generate a report.
User Profile Type	Displays the profile type of the user with defined access on Role, Group, or Service.

Table 40. Filters for the User Access report - View by User report type (continued)

Parameter	Description
User Name	Displays the full name of the user from a business unit.

Select the values for these parameters, then click **Finish** to generate the report.

The Prompt Page Summary provides an overview of the report parameters and the selected values. The next page lists all of the users that you filtered, with their details and sorted based on their business unit.

Click the *User Name* link to view all access corresponding to the selected user.

User Recertification History Report

Use this report to view the recertification history for a user. This report covers the recertification audit history of accounts, groups, and roles that are associated with the user.

After you select the values for these parameters, the Prompt Page Summary is generated. The Prompt Page Summary provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 41. Filters for User Recertification History Report

Parameter	Description
Start Date	Displays the start date of user recertification history.
End Date	Displays the end date of user recertification history.
User Recertification Policy	Displays information about the user recertification policy.
User Business Unit	Displays the business unit name of a user.
User	Displays the user from a business unit.
User Status	Displays status of the user to be selected.
Recertifier	Displays user to be selected as recertifier.

Defining the base icon URL path

You must define the base icon URL path in query of the Access Definition Report or User Access Report to display the icon in the report.

About this task

IBM Security Identity Manager provides a way to define an icon URL for an access. The icon URL can be either a relative path or an absolute path. Assume that a user defined the icon URL `"/images/icons/test.gif"` in IBM Security Identity Manager. To display the actual image for the icon URL, IBM Cognos application must locate the full path for that image. In such a situation, you must define the base icon URL path in the query of the access definition report.

Procedure

1. Open the report in **Report Studio**.
   a. Access `https://hostname:port/ibmcognos/cgi-bin/cognos.cgi`.
   b. In IBM Cognos Connection window, click **ISIMReportingModel_6.0.0.3**.

c. Select the report, which is applicable.
   - **Access Definition Report** or
   - **User Access Report**

d. Under **Actions** column, click **Open with Report Studio**.

2. Click **View** > **Queries** to open the Query Explorer.
3. Double-click **Access Query**.
4. In the Data Items window, double-click **Base Icon URL**.
5. In the Expression Definition window, set the base URL for the icons. For example, `'http://xyz.com'`.
6. Click **OK**.
7. Save the report.

What to do next

Run the report to display the icons.

Query subjects and query items for the report models

Use the query subjects and query items information to customize the IBM Security Identity Manager reports.

Schema mapping

Before you work with the query subjects and query items, you must map the attributes to the entities.

For more information, see "Report schema mapping" on page 325.

To map the attributes and entities, see "Mapping the attributes and entities" on page 299.

`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 42. 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.

Table 42. Query subjects in the `Recertification Audit` namespace for the recertification model (continued)

Query subject	Description
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 43. 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 43. 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 43. 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 43. 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 43. 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 43. 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 43. 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 43. 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 44. 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 45. 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 45. 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 45. 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 45. 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 45. 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 45. 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.

Use the account audit model and reports to view the details about the accounts that are associated with a user.

Note: If the account is on the service that is defined as an access, the audit details can be seen only in the `Access Audit` namespace.

Query subjects for `Account Audit` namespace:

The following table lists the query subjects in the `Account Audit` namespace.

Table 46. 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 47. 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 47. 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 47. 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 47. 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 48. 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 48. 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 49. 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 49. 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 49. 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 49. 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 49. 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 49. 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. • `ITIMService` - 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 49. 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 49. 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 50. Query subjects in the `Provisioning Policy Audit` namespace

Query subject	Description
Provisioning Policy Audit	Represents a history of the provisioning policies and accounts.

Table 50. 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 51. 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 51. 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 52. 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 53. 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 53. 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 53. 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 54. 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 54. 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 55. 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 55. 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 55. 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 56. 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 56. 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 57. 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 57. 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 57. 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 57. 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 57. 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 57. 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 58. 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 59. 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 59. 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 59. 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 59. 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 59. 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 60. 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.
Separation of Duty Rule	Represents the separation of duty rule that is associated with the separation of duty policy.

Table 60. Query subjects in the Separation of Duty Configuration namespace (continued)

Query subject	Description
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 61. 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 61. 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 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 62. 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.

Table 62. Query subjects in the User Configuration namespace (continued)

Query subject	Description
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.
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.
User	Represents all users of type *person* and *business partner person*. Use this query to get a consolidated view of all users that are defined in the organization. You can use this query subject with the **Person** and **Business Partner Person** query subjects to retrieve more specific details about the user.

Query items for User Configuration namespace:

The following table lists the query items in the User Configuration namespace.

Table 63. 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.

Table 63. List of query items in the `User Configuration` namespace (continued)

Query subject	Query items and their description
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.
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 63. 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 63. 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 63. 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 63. 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 63. 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 63. 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.
User	**Full Name** The full name of the user. **Last Name** The surname of the user. **Type** The profile type of the user, which is either *person* or *business partner person*. **Status** The status of the user, which is either *Active* and *Inactive*. **Supervisor** The supervisor of the user. **Business Unit Name** The name of the business unit to which a user belongs. **Dn** An LDAP distinguished name for a user. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs.

`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 64. 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 65. 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 65. 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 65. 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(Deprecated) namespace

The Access Audit(Deprecated) namespace pertains to the audit history of the actions that are performed on the access entities. The access audit is supported for the group, role, and service that is defined as an access.

Query subjects for Access Audit(Deprecated) namespace:

The following table lists the query subjects in the Access Audit(Deprecated) namespace.

Table 66. Query subjects in the Access Audit(Deprecated) 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(Deprecated) namespace:

The following table lists the query items in the Access Audit(Deprecated) namespace.

Table 67. List of query items in the `Access Audit(Deprecated)` 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 67. List of query items in the `Access Audit(Deprecated)` 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 67. List of query items in the `Access Audit(Deprecated)` 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 67. List of query items in the Access Audit(Deprecated) 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 Audit namespace

Use the access audit model and reports to view the details about the accesses that are associated with a user.

The Access Audit namespace pertains to the audit history of the actions that are performed on the access entities in Identity Service Center. The access audit is supported for the group, role, and service that is defined as an access.

Note: If the account is on the service that is defined as an access, the audit details can be seen only in the Access Audit namespace.

Query subjects for Access Audit namespace:

The table lists the query subjects in the Access Audit namespace.

Table 68. Query subjects in the Access Audit namespace

Query subject	Description
Access Audit	The audit history of the access entity. You must use this query subject with the Access query subject.
Access Audit Obligation Attributes	The obligation attributes of an access and their values. You must use this query subject with the Access Audit query subject.
Access	The access entity on which the audit actions are performed. This query subject also contains the configuration attributes of an access.
Access Owner	A user who owns the access.

Query items for Access Audit namespace:

The table lists the query items in the Access Audit namespace.

Table 69. 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 Action** An action that is run on the access. The valid values are Add, Edit, or Delete. **Audit Comments** The comments that are entered by the audit workflow approver. **Audit Initiator Name** The name of a user who initiates the audit action. For the audit actions such as Add, Edit, or Delete, the initiator name represents the name of IBM Security Identity Manager account. **Audit Account ID** An account identifier of a user for whom the access is requested. **Audit Access Requestee Name** The name of a user whose account is added to the access. **Audit Access Approver Name** The name of a user who approves the audit action. **Audit Access Approver Account ID** An account identifier of an audit approver. **Audit Access Business Unit** The name of an audit access business unit. **Audit Workflow Process ID** A unique identifier for a workflow process that is associated with the access request. **Audit Operation Start Time** The audit operation start date and time. **Access Type Code** The code for an audit entity type. The possible values are 1, 2, and 3. 1 represents service, 2 represents group, and 3 represents role. **Audit Access Type** The type of an access. For example, Application, Role, Email group, or Shared Folder. **Audit Access Badge Text 1, Audit Access Badge Text 2, Audit Access Badge Text 3, Audit Access Badge Text 4, Audit Access Badge Text 5** The badge text that is defined for an access. **Audit Access ID** A unique identifier of an access on which the audit operation is run.

Table 69. List of query items in the `Access Audit` namespace (continued)

Query subject	Query items and their description
Access Audit (Continued)	**Audit Access Request Justification** The reason for the access request. **Audit Activity Name** The name of an audit activity. **Audit Activity ID** A unique identifier of an audit activity. **Audit Activity Start Time** The audit activity start date and time. **Audit Activity Due Time** The date and time when the audit activity is due for an approval. **Audit Activity Escalation Time** The escalation date and time of an audit activity. **Audit Activity Completion Time** The audit activity completion date and time. **Audit Access Request Completion Time** The date and time when an access request is completed. **Audit Access Request Status** The status of an access request. The possible values are `Fulfilled`, `Not Fulfilled`, `Submitted`, or `Pending`. **Audit Activity Approval Status** An approval status of an audit activity. For example, `Approved`, `Rejected`, or `Pending`. **Audit Activity Approval Action** The status of an action that is taken on the activity. For example, `Completed` or `Escalated`. **Audit Action Code** A code for the audit action. the possible values are `ADD`, `CHANGE`, or `DELETE`. **Access Audit Obligation ID** A unique obligation identifiers of an access. There can be multiple obligation identifiers that are separated by a comma.
Access Audit Obligation Attributes	**Access ID** A unique identifier of an access on which the audit operation is run. **Access Audit Obligation ID** A unique obligation identifier of an access. **Access Account Attribute Name** The attribute name of an account that belongs to the access. **Access Account Attribute Previous Value** The previous value of an account attribute that belongs to an access. If the attribute is edited for the first time, the previous value is empty or null. **Access Account Attribute Modified Value** The modified value of an account attribute that belongs to an access.

Table 69. List of query items in the Access Audit namespace (continued)

Query subject	Query items and their description
Access	**Access Dn** An LDAP distinguished name for an access. **Access Name** The name of an access. **Access Type** The type of an access. The possible values are Group, Role, or Service. **Access Description** The description of an access. **Access Category** A category of an access. For example, Application, Role, Email Group, or Shared Folder. **Access Icon URL** A URL that is defined for an access icon. **Access Additional Information** An additional information about the access. **Access Enabled** Specifies whether access is enabled. The possible values are True and False. **Access Common Enabled** Specifies whether common access is enabled. The possible values are True and False.
Access Owner	**Access Dn** A distinguished name of an access. **Access Owner Dn** A distinguished name for an access owner. **Access Owner** The name of an access owner. **Access Owner Type** The type of an access owner. For example, Person or Role. **Access Owner Status** The status of an access owner. For example, Active and Inactive. The access owner status is not applicable if an owner type is a role. **Access Owner Manager Dn** A distinguished name for a manager of an access owner. **Access Owner Business Unit** The business unit name of an access owner. **Access Owner Business Unit Dn** A distinguished name for a business unit of an access owner.

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 70. 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. **Note:** Group information is displayed if group access is set to enabled or common access enabled.
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. **Note:** Role information is displayed if role access is set to enabled.
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 all users of type *person* and *business partner person*. Use this query to get a consolidated view of all users that are defined in the organization. You can use this query subject with the **Person** and **Business Partner Person** query subjects to retrieve more specific details about the user

Query items for Access Configuration namespace:

The following table lists the query items in the Access Configuration namespace.

Table 71. List of query items in the Access Configuration namespace

Query subject	Query items and their description
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 Dn** An LDAP distinguished name for 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.
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 Status** Provides the state of access definitions. For example: access is enabled, or common access is enabled. **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 Search Terms** Displays the search string for a service defined as an access.

Table 71. List of query items in the `Access Configuration` namespace (continued)

Query subject	Query items and their description
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.
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 Status** Provides the state of access definitions. For example: access is enabled, or common access is enabled. **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. **Access Search Terms** Displays the search string for a group defined as an access.

Table 71. 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 the user. **Last Name** The surname of the user. **Type** The profile type of the user, which is either *person* or *business partner person*. **Status** The status of the user, which is either *Active* and *Inactive*. **Supervisor** The supervisor of the user **Business Unit Name** The name of the business unit to which a user belongs. **Dn** An LDAP distinguished name for a user. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs.
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.

Table 71. 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 Status** Provides the state of access definitions. For example: access is enabled, or common access is enabled. **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. **Access Search Terms** Displays the search string for a role 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.

Table 71. List of query items in the `Access Configuration` namespace (continued)

Query subject	Query items and their description
User	**Full Name** The full name of the user. **Last Name** The surname of the user. **Type** The profile type of the user, which is either *person* or *business partner person*. **Status** The status of the user, which is either *Active* and *Inactive*. **Supervisor** The supervisor of the user **Business Unit Name** The name of the business unit to which a user belongs. **Dn** An LDAP distinguished name for a user. **Business Unit Dn** An LDAP distinguished name for the business unit to which a user belongs.

References

Reference information is organized to help you locate particular facts quickly, such as the mapping attributes, entities, or scenario to configure the report model.

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 72. Mapping the attributes and entities

Namespace	Entity	Attribute Name
`Account Audit`	`Business partner person`	`Status`
`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`
	`Business partner person`	`Status`

Table 72. 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
	Business partner person	• Full name • Last name • Parent DN • Sponsor
Recertification Audit	Account	Account Ownership Type
Recertification Config	Account	Account Ownership Type
	Group	• Access description • Group description • Group name
	Recertification policy	Scope
User Audit	Business partner person	Status
User Configuration	Account	Account Ownership Type
	Person	• Administrative Assistant • Preferred user ID • E-mail address • Aliases
	Organizational Role	• Access Name • Access Options • Object profile name • Owner
	Business partner person	• Organizational roles • 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 • Organizational roles • Status
	Person	• Organizational roles

Report model configuration by using IBM Cognos components

To customize reports, you might be required to configure the report model. The following table provides a list of the basic tasks for configuring any IBM Cognos report model. It also provides information about the user guide for some IBM Cognos components.

Table 73. Basic tasks to configure report model

Tasks	**Access the IBM Cognos Business Intelligence 10.2.1 documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html**
Framework Manager user guide.	Search for **Framework Manager User Guide 10.2.1**.
Query Studio user guide.	Search for **Query Studio User Guide 10.2.1**.
Report Studio user guide.	Search for **Report Studio User Guide 10.2.1**.
Cognos Connection user guide.	Search for **Cognos Connection User Guide 10.2.1**.
Import the metadata from the relational database.	Search for **Importing metadata from relational databases**.
Create a relationship.	Search for **Creating relationships**.
Modify a relationship.	Search for **Modifying a relationship**.
Create a complex expression for a relationship.	Search for **Creating complex expressions for a relationship**.
Create a data source query subject.	Search for **Data source query subjects**.
Create a model query subject.	Search for **Model query subjects**.
Update query subjects.	Search for **Updating query subjects**.
Create or modify a package.	Search for **Creating or modifying packages**.
Publish a package.	Search for **Publishing packages**.

Migration of Tivoli Common Reporting reports to IBM Cognos reports

You can use the reference of the following link to convert Tivoli Common Reporting reports to IBM Cognos reports.

The following link provides information about converting the Business Intelligence and Reporting Tools (BIRT) reports to IBM Cognos reports. You can obtain the reference by using the following link to convert Tivoli Common Reporting reports to IBM Cognos reports. See http://www.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ttcr_converting_birt_to_cognos.html.

Scenarios

See the possible scenarios that can be used to customize the IBM Security Identity Manager Cognos report model.

Adding custom tables:

The scenario describes the steps to add or import custom tables in IBM Security Identity Manager Cognos model.

Before you begin

- Install and configure IBM Cognos Business Intelligence server.
- Install IBM Framework Manager.
- Map the user and its required attributes through schema mapper in IBM Security Identity Manager Console and run the data synchronization.

About this task

You can define the custom types or objects in IBM Security Identity Manager. By default, IBM Security Identity Manager provides the objects `Person` and `Business Partner Person` for a `User` entity. You can further define your own object classes that can be used as the custom person or custom Business Partner person types. For example, `JKPerson`.

Consider that a custom user `JKPerson` defined in IBM Security Identity Manager. With this customization in IBM Security Identity Manager, there are two profiles or types of a user. The `Person` is a type that is provided by default and a new customized person `JKPerson`.

Procedure

1. Extract the `ISIMReportingModel_6.0.0.6.zip` to the local disk.
2. Create a project in IBM Cognos Framework Manager and open `.cpf` file for the model customization.

   Note: Open an existing project if any customization is already done in IBM Security Identity Manager metadata model.
3. Navigate to the **Database Layer**.
4. Select the **Database Layer**.
5. Right click, and then select **Run Metadata Wizard**.
6. Select `ISIM` as a data source from the list that is defined in IBM Cognos, and then click **Next**.
7. Select the objects that you want to import, and then click **Next**. For example, `JKPerson`, `JKPerson_CN`, or `JKPerson_SN`.
8. On **Generate Relationships** panel, clear the **Use primary and foreign keys** check box.
9. Click **Import**.

Results

`JKPerson`, `JKPerson_CN`, or `JKPerson_SN` are added to the database layer in metadata model. Similarly, you can import the other required tables that you want.

Creating a relationship with the existing tables:

The scenario describes the steps to create a relationship with any existing custom table.

Before you begin

- Install and configure IBM Cognos Business Intelligence server.
- Install IBM Framework Manager.
- Map the user and its required attributes through schema mapper in IBM Security Identity Manager Console and run the data synchronization.

About this task

IBM Security Identity Manager Cognos report model is divided into two basic namespaces: audit and configuration. Audit namespace provides the tables or query subjects that helps to generate the audit reports. Configuration namespace provides the configuration information that helps to generate configuration reports.

You can define the custom types or objects in IBM Security Identity Manager. By default, IBM Security Identity Manager provides the objects Person and Business Partner Person for a User entity. You can further define your own object classes that can be used as the custom person or custom Business Partner person types. For example, JKPerson.

The JKPerson is of a type User. Therefore, navigate to the User configuration namespace to merge the JKPerson.

Procedure

1. Extract the ISIMReportingModel_6.0.0.6.zip to the local disk.
2. Create a project in IBM Cognos Framework Manager and open .cpf file for the model customization.

   Note: Open an existing project if any customization is already done in IBM Security Identity Manager metadata model.
3. Navigate to the **Database Layer**.
4. Hold the **Ctrl** key, and select the JKPerson and JKPerson_CN tables.
5. Right click, and then select **Create** > **Relationship**.
6. Set the **Cardinality**, and then click **OK**.
7. Create a relationship between the JKPerson and JKPerson_SN tables
8. A common entity such as User lists all types of the users. For example, Person, Business Partner Person, or JKPerson.

   To create a common entity, pick the common attributes in them. Assuming that the cn, sn, businesunit dn, and dn are the attributes that are must, create the JKPerson Must Attributes query subject that contains the attributes that are must. Rename an individual item to some business names. For example, CN to Full Name, SN to Last Name.

   Introduce one more data item as Type. The Type attribute indicates the type of a user such as JKPerson.

   a. Navigate to the **Database Layer**.
   b. Select the **Database Layer**.
   c. Right click, and then select **Create** > **Query subject**.
   d. Select the type as a Model query subject.
   e. Provide the name to the query subject. For example, JKPerson Must Attributes.
   f. Click **OK**. The **Query Subject Definition** window is displayed.
   g. Navigate to the **Database Layer**.
   h. Add JKPerson DN, Business Unit Dn from the JKPerson query subject.
   i. Add JKPerson_CN from the JKPerson_CN and JKPerson_SN from the JKPerson_SN.
   j. Add a Type data item to indicate the type of a user.
      1) Click **Add** link.
      2) Provide the **Type** as a name to the item.
      3) In the expression definition, add the JKPerson.
      4) Click **OK**.
9. Edit the union definition for the User query subject and include newly added JKPerson Must Attributes query subject.
10. Select User, right click, and test the results.

11. Optional: Create a shortcut of User and use it in the namespace. For example, User Configuration.
    a. Select a User from the database layer.
    b. Right click, and select **Create** > **Shortcut**.
    c. Drag the shortcut to User Configuration namespace.
    d. Rename the shortcut query to JKPerson or some business name and use it as per the requirement.

Results

The relationship is created with the existing tables.

Adding custom attributes to an existing query subject:

The static report does not show an email address. You can configure the report model to add custom attributes such as, an email address. The scenario describes how to configure model so that you can view or drag the email addresses of the users in the reports.

Before you begin

- Install and configure IBM Cognos Business Intelligence server.
- Install IBM Framework Manager.

Procedure

1. Add the E-mail property to the ISIM database schema.
    a. In the IBM Security Identity Manager console, select **Reports** > **Schema Mapping**.
    b. From the **Entities** list, select **Person** entity.
    c. From the unmapped attribute list, select **E-mail address**.
    d. Click **Add**.
2. Run the data synchronization tool.
    a. Select **Reports** > **Data Synchronization**.
    b. Click **Run Synchronization Now**.
3. Add the information about email address in the ISIMReportingPackage_6.0.0.6.zip.
    a. Open the Framework Manager.
    b. Extract the ISIMReportingModel_6.0.0.6.zip to the local disk.
    c. Open the .cpf file in the ISIMReportingModel_6.0.0.6 folder.
    d. Right click the IBM Identity Security Manager (ISIM) namespace and select **Run Metadata Wizard**.
    e. From the Metadata Wizard window, select **Data Source** and click **Next**.
    f. Select **ISIM** and click **Next**. You must use the data source name as **ISIM**.
    g. Select the ITIMUSER object and click **Tables**.
    h. Select the PERSON_MAIL table and click **Next**.
    i. Clear the **Use primary and foreign keys** check box.
    j. Click **Import**.
    k. Click **Finish**.
4. Create a relationship between the PERSON and PERSON_MAIL table.
    a. Hold the Ctrl key and select the PERSON and PERSON_MAIL tables.

b. Right click and select **Create** > **Relationship**.
c. Set the **Cardinality** of the following items:
   - `PERSON` table to 1..1
   - `PERSON_MAIL` table to 0..1
d. Click **OK**.

5. Publish the modified model.
   a. In the Framework Manager console, expand **Packages**.
   b. Right click the metadata model and click **Publish Packages**.
   c. Click **Next** twice.
   d. Click **Publish**.
   e. If the package was published previously, a message prompts for the confirmation. Click **Yes**.
   f. Click **Finish**.

Results

You can view the email addresses in the reports.

Troubleshooting report problems

The following section describes solutions for the IBM Security Identity Manager Cognos report problems.

Problems and their solutions

Unable to view the IBM Security Identity Manager Cognos drill through reports in Microsoft Internet Explorer version 10

If you are using the Microsoft Internet Explorer version 10 browser, the IBM Security Identity Manager Cognos drill through reports might not work.

Solution

Complete the following steps:

1. Enable the compatibility view.
   a. In the Microsoft Internet Explorer 10 menu, go to **Tools**.
   b. Select **Compatibility View**.
2. Add the IBM Cognos website to the trusted sites list.
3. In the Microsoft Internet Explorer 10 menu, go to **Tools** > **Internet Options**.
4. On the **Security** tab, click the **Trusted sites** icon.
5. Click **Sites**.
6. In the **Add this website to the zone** box, add the IBM Cognos website address.
7. Click **Add**.
8. Click **Close**.

IBM Cognos audit history report does not show the audit of an account that is provisioned on the managed resource

IBM Cognos audit history for an account does not show the audit of the account that is provisioned on the managed resource when "Default Account Request Workflow" is configured with the entitlements that are associated with the provisioning policy.

Solution

To generate the audit history reports for the accounts with the default workflow, clear the **Approval Start Date** and **Approval End Date** check boxes, and then run the report.

IBM Security Identity Manager Cognos report execution fails on Oracle data source During the report generation on Oracle data source, if you select more than 1000 filter values on the prompt page, the report execution fails.

Solution

1. Open the report in IBM Cognos Report Studio.
2. Open the prompt page and edit the property **Rows Per Page** for all input widgets.
3. Set the value to less than or equal to 1000.

The scope for the default provisioning policy is shown as blank on Oracle database.

When you generate the customized IBM Cognos report that includes provisioning policy scope in it, the scope for the default provisioning policy is shown as blank. This issue is specific to Oracle database.

Solution

If the scope for the default provisioning policy is shown as blank on Oracle database, then, interpret the scope of a provisioning policy as `Subtree`.

No data is displayed in the IBM Security Identity Manager Cognos audit history report Account audit is not supported for an account that is added and does not have a defined workflow. To audit the accounts for an audit history report, the default workflow or custom workflow must be attached to the provisioning policy that is created.

Long filter values are not shown completely on the prompt pages

Follow the technote link http://www-01.ibm.com/support/docview.wss?uid=swg21341018 to resolve this issue. The information in the technote also applies to IBM Cognos Business Intelligence version 10.2.1 Fix Pack 1.

Known limitations

The Prompt Page Summary table in the IBM Cognos Report shows "--" as the parameter value when more than 1000 filters per prompt is selected.

IBM Cognos Reports provide the option for multiple selection. You can select more than one value for each parameter in the prompt page. When you select several values to filter the report, text overflow can occur and '--' is displayed instead in the Prompt Page Summary table.

Solution

Avoid selecting too many values for each parameter in the prompt page.

IBM Cognos Reports do not display the actual values of custom labels that are defined in the Custom Labels properties file

IBM Security Identity Manager supports the use of custom labels. You can specify these labels in the `CustomLabels_<locale>.properties` file. Custom labels are defined in a key-value pair format. This key can be used to set custom access types, access badges, and others.

For example:

- *Custom access badge label:* `$OPDData`
- *Custom access badge label value:* `Critical`

You can view the access catalog information or entitlements from the following IBM Security Identity Manager reports:

- Access Definition Report
- User Access Report

These reports list all access that is defined in the IBM Security Identity Manager console. When you define an access badge in the IBM Security Identity Manager console, the value can be:

- Derived from the `CustomLabels_<locale>.properties` file. For example: `$OPDData` OR
- A regular string value. For example: `"Sensitive data"`

For custom labels, these reports display the key for the respective label. For example: `$OPDData`. You must see the `CustomLabels_<locale>.properties` file to get the actual value of the custom label.

Disabled access is not displayed in the User Access Report

The access that is defined on groups and roles cannot be displayed in the User Access Report if the access is disabled.

User entitlements are not displayed in Legacy Administrator console reports and in BIRT reports

Both the Legacy Administrator console reports and BIRT reports do not show the entitlements that are granted to an individual when the provisioning policy membership is set to "All Other Users". To resolve the problem, use Cognos-based entitlements granted to an individual report to get the entitlement details.

Audit of the disconnected credentials in the IBM Cognos shared access history report

In IBM Security Identity Manager, a user can disconnect the shared access credentials in the credential vault. After the credentials are disconnected, the credentials in the vault do not have a connection with an account.

IBM Cognos shared access history report does not include the check-out and check-in history of the credentials that are not connected to an account. The shared access history report does not show the disconnected credentials for check-out and check-in audit action.

IBM Cognos entitlements report shows the provisioning policy data that is in the draft state

The IBM Cognos entitlements report shows the entitlements that are granted to an individual. It lists all the users and the items for which they are entitled. The report also shows the provisioning policy information that includes the policies that are saved in the draft state.

Cannot truncate the length of the text in the pie charts

An option or a property that can be set to truncate the length of the text is not available for the pie charts. You cannot truncate the length of the text in the pie charts.

Languages that are not supported by the IBM Cognos Business Intelligence Server version 10.2.1 Fix Pack 1

IBM Cognos Business Intelligence Server version 10.2.1 Fix Pack 1 does not support the following languages:

- ar=Arabic
- iw=Hebrew

It provides partial support for the following language:

- el=Greek

  The IBM Cognos Business Intelligence Server 10.2.1 Fix Pack 1 is not fully translated into the Greek language. Only components like `Cognos Viewer`, `Cognos Connection`, `Cognos Administration`, and `Cognos Workspace` support translation in the Greek language.

Note: The unsupported languages are not in the **Product Language** list, although they are displayed in the **Content Language** list in the Cognos configuration of IBM Cognos Business Intelligence Server.

Duplicate entries of the account add operation are observed when you run the account audit report

Duplicate entries of the account add operation are observed if the provisioning policy is configured with the default workflow and an extra custom workflow is created in IBM Security Identity Manager Console under **Configure System** > **Manage Operations**.

Solution

Remove the default workflow that is defined in the provisioning policy. Therefore, only the custom workflow that is defined would be effective, which would be captured in the account audit report.

Custom workflows that are defined in IBM Security Identity Manager are not supported for the following type of actions on an account

Only the default workflows are supported for the following actions on an account.

- Restore
- Suspend

Audit of the custom access type is not supported in the access audit history report Any custom access type that is defined as access for a role, service, or group cannot be audited in the access audit history report.

IBM Security Identity Manager console reports

The section provides information about IBM Security Identity Manager console reports.

Types of reports

View descriptions of the reports that you can generate for IBM Security Identity Manager.

Requests

Account Operations

A report that lists all account requests. Allows filtering by account operation, service, and other fields.

Account Operations Performed by an Individual

A report that lists account requests made by a specific user. Allows filtering by the user who made the request in addition to other fields.

Approvals and Rejections

A report that lists request approval activities that were approved or rejected. Allows filtering by activity approver, service, and other fields.

Operation Report
A report that lists all operations submitted in the system. Allows filtering by requestee, operations, and the request start date and end date.

Pending Approvals
A report that lists the request activities submitted but not yet approved. Allows filtering by service, activity status, and other fields.

Rejected Report
A report that lists all rejected requests. Allows filtering by requestee and the request start date and end date.

User Report
A report that lists all requests, shows the set of operations that were requested, who the operations were requested for, and who requested them. Allows filtering by requestor, requestee, and the request start date and end date.

User and Accounts

Account Report
A report that lists accounts for a business unit. Allows filtering by service and business unit.

Accounts/Access Pending Recertification Report
A report that lists all pending recertifications for access definitions and accounts. Allows filtering by account or access owner, service type, and service.

Individual Access
A report that lists user access definitions selected by individual account owner, business unit, access, or service. Allows filtering by a user that owns accesses, business unit of the user, access defined in the system, and service where access is supported.

Individual Accounts
A report that lists the accounts and their owners. Allows filtering by user.

Individual Accounts by Role
A report that lists accounts owned by users of a specific role that is a member of provisioning policy. Allows filtering by role and business unit.

Recertification Change History Report
A report that lists the recertification history of accounts and user accesses. Allows filtering by account or access owner, recertification response, start date and end date, and other fields.

Suspended Individuals
A report that lists all individuals that are suspended. Allows filtering by date.

Services

Reconciliation Statistics
A report that lists the activities that occurred during the last completed reconciliation of a service, regardless of when the report data was synchronized. Remote services provide reconciliation statistics during a reconciliation. This report contains data from the

last service reconciliation. Data synchronization is not a report prerequisite. Allows filtering by service.

Services
A report that lists services currently defined in the system. Allows filtering by service type, service, owner and business unit.

Summary of Accounts on Service
A report that lists the accounts on a specified service. Allows filtering by service and account status.

Audit and Security

Access Control Information (ACIs)
A report that lists all access control items in the system. Allows filtering by access control item name, protection category, object type, scope, and business unit.

Access Report
A report that lists all access definitions in the system. Allows filtering by access type, access entitlement, service type, service, and administration owner of an access definition.

Audit Events
A report that lists all audit events. Allows filtering by audit event category, action, initiator, start date, and end date.

Dormant Accounts
A report that lists the accounts that have not been used recently. An account that does not have last access information is not considered dormant, including new accounts where the last access date is blank. These types of accounts are not displayed in a dormant report. Allows filtering by service and dormant period.

Entitlements Granted to an Individual
A report that lists all users with the provisioning policies for which they are entitled. Allows filtering by user.

Note: This report shows direct entitlements and not inherited entitlements.

Non-Compliant Accounts
A report that lists all accounts that are noncompliant. Allows filtering by service and the reason for noncompliance.

Orphan Accounts
A report that lists all accounts that do not have an owner. Allows filtering by service and account status.

Policies
A report that lists target and memberships of the provisioning policies in the system. Allows filtering by policy name.

Policies Governing a Role
A report that lists all provisioning policies for a specified organization role. Allows filtering by role name.

Recertification Policies Report
A report that lists all recertification policies. Allows filtering by policy target type, service type, service, access type, and access.

Suspended Accounts
A report that lists the accounts that are suspended. Allows filtering by user, account, service, and date.

Generating reports

You can generate reports based on requests, user and accounts, services, or audit and security.

Before you begin

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

About this task

Reports of subsets of information can help you discover trends that can help you identify ways to improve your business process.

To generate a report, select the type of report you want to generate, and specify the criteria of the report. The criteria you specify depends on the type of report and controls the scope and quantity of the report entries.

To generate a custom report, you must first create the report schema that specifies what entities and attributes can be made available for the custom report.

Generating requests reports

Generate the reports that provide workflow process data.

Before you begin

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

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports** > **Requests Reports**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Generating user and accounts reports

Generate the reports that provide user and accounts data.

Before you begin

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

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports** > **User and Accounts Reports**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Generating services reports

Generate the reports that provide service data.

Before you begin

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

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports** > **Services**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Generating audit and security reports

Generate the reports that provide audit and security data.

Before you begin

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

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports** > **Audit and Security Reports**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Regular expression notation usage for searching

Regular expression notation is a group of symbols and characters that make up a syntax that is used as a template to match patterns of text.

Note: The Report task in the console supports only the wildcard (*) as a regular expression character. If you select the **Search** function in the console while you are doing a report-related task, you can specify only the wildcard as a regular expression character.

If a regular-expression field displays an asterisk (*) as the default character, that character is interpreted as a wildcard character that indicates that all string values apply. No filtering is done to reduce the number of string values that apply. IBM Security Identity Manager supports the set of regular expression characters from Java (regex4j).

Regular expressions are commonly used on UNIX platforms and in the PERL 5 language. A free online tutorial, *Using regular expressions*, is available on the following IBM developerWorks® website:

http://www.ibm.com/developerworks/java/

Type `regular expression` in the **Search for** field when the website is displayed, and then select **Using regular expressions** from the list of topics. You must register with developerWorks to take the tutorial.

Report customization

Use the `Design Report` task to create report templates. Add them to a table that contains a selection of report templates that you can modify or delete.

When you, as an administrator, create a custom report, you must also manually create report ACIs and entity ACIs for that custom report. The ACIs allow users that are not administrators, such as auditors, to run the custom report and to view data in the custom report.

Report templates can apply to one of the following categories. The category determines where the reporting link is displayed in the task portfolio.

- Requests
- User and Accounts
- Services
- Audit and Security
- Custom

Report templates

All reports, including standard reports and custom reports, are generated with report templates. A *report template* defines the layout of a report and the filter criteria that determines the contents of the report. When you select a report to run, you are selecting the report template used to generate the report.

IBM Security Identity Manager provides a large set of standard report templates that are designed to help you manage system resources and monitor the status of various activities and accounts. You can keep the standard report templates in their original form to generate reports. You can also examine them to determine how to design custom report templates, or modify the standard report templates to meet the needs of your organization. You modify standard report templates with the Design Report task in the console.

Custom reports are generated with report templates that you design. Use either the built-in report designer or a third-party report designer.

When you use the Design Report task, you can determine which report designer was used to create the report template. Use the **Report Type** column in the reports table. **Designer** identifies report templates that were created with IBM Security Identity Manager Design Report task. You can modify these report templates with Design Report task.

Creating custom report templates

Use the IBM Security Identity Manager report designer to create custom report templates.

Before you begin

Run the data synchronization process before you create a custom report template. See “Data synchronization for reports” on page 337.

Procedure

To create a custom report template, complete these steps:

1. From the left navigation pane, select **Reports** > **Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.

5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

   Important: You must add at least one column to create the report.
10. Complete the following steps on this page:
    a. From the **Apply Case** list, select an appropriate option.
    b. From the **Entity** list, select an appropriate option. For example, select **Role Assignment Attributes**.
    c. From the **Attribute** list, select one of the options for adding it as a column in the report. For example, select **Attribute Name**.

       Note: Attribute list options are mapped with the entity that you selected earlier.
    d. In the **Column width** field, type the size of the column. The default value is 5.
    e. In the **Sort** section, complete these steps:
       - Select one of these options: **None**, **Ascending**, or **Descending**.
       - From the **Sort order** list, select an appropriate option. For example, **2**.
    f. Click **OK** to add the column in the report.
11. Click the **Filter** tab, and then add or remove rows and columns for the report according to your requirements. For example, you can add a row in the report for a list of roles that have assignment attributes. To do so, complete these steps under the **Add a New Filter Row** area:
    a. From the **Entity** list, select **Organizational Role**.
    b. From the **Attribute** list, select **DN**.
    c. From the **Operator** list, select **Equals**.
    d. From the **Entity** list, select **Role Assignment Attributes**.
    e. From the **Attribute** list, select **Role Distinguished Name**.
    f. From the **Condition** list, select one of these options:
       - None: Indicates that no more filter condition can be added to the report.
       - AND: Generates results only if all the specified filter conditions meet.
       - OR: Generates results if either of the specified filter conditions meet.
12. Optional: Click **Preview** to open a new browser window that contains a preview of the report.
13. Click **OK** to create the custom report.

Results

A message is displayed, which indicates that you created the custom report template.

What to do next

Generate the custom report that you created either in a PDF or a CSV format. See "Generating custom reports" on page 317.

Modifying custom report templates

Use the report designer to modify custom reports that you created.

Before you begin

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

About this task

To modify a custom report template, complete these steps:

Procedure

1. Click **Reports** > **Design Report**. The Custom Report Template page is displayed, which contains a table that lists the standard report templates. The table might consist of multiple pages.
2. On the Custom Report Template page, click the name of the report that you want to modify. The General tab of the Design Report notebook is displayed.
3. On the General tab, modify the fields as wanted, and then click the **Contents** tab. The Contents tab of the Design Report notebook is displayed.
4. Optional: On the Contents tab, add attributes to the report column as follows:
   a. Click **Add** to add an attribute as a column of data in the report. The Report Column Details page is displayed.
   b. On the Report Column Details page, complete the fields as wanted, and then click **OK**. The new attribute is displayed in the **Report Column** of the attribute table that is within the Contents tab.
5. Optional: On the Contents tab, remove attributes from the report column as follows:
   a. Select the check box next to the attribute that you want to remove. Selecting the check box at the top of this column selects all attributes.
   b. Click **Remove**. The table on the Contents tab is refreshed, and the attribute is removed.
6. Click the **Filter** tab. The filter for the report template is displayed.
7. On the Filter tab, select the row in the list box to view the filter details. Filters cannot be modified for out-of-box reports. Only the filters of custom-designed report can be modified.
8. Click **Preview** to open a new browser window that contains a preview of the report, or click **OK** to save the report template.

Results

A message is displayed, indicating that you successfully updated the report template.

What to do next

To view the updated report template within the custom report table, click **Return to the Report Design Page**. You can also select another reporting task, or click **Close**.

Deleting custom report templates

Use the report designer to delete custom report templates that you no longer need.

Before you begin

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

About this task

To delete a custom report template, complete these steps:

Procedure

1. Click **Reports** > **Design Report**. The Custom Report Template page is displayed, which contains a table that lists the standard report templates. The table might consist of multiple pages.
2. On the Custom Report Template page, select the check box next to the report template that you want to delete. Selecting the check box at the top of this column selects all report templates.
3. Click **Delete**. A confirmation page is displayed.
4. On the Confirm page, click **Delete** to delete the selected report template, or click **Cancel**.

Results

A message is displayed, indicating that you successfully deleted the report template.

What to do next

To view the custom report table, click **Return to the Report Design Page**. You can also select another reporting task, or click **Close**.

Generating custom reports

Generate the custom reports that are designed with the `Design Report` task.

Before you begin

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

About this task

Custom reports can be located within any of the report categories and not necessarily only in Custom Reports.

To generate a custom report from the Custom Reports category, complete these steps:

Procedure

1. Click **Reports** > **Custom Reports**.
2. Click the name of the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Shared access objects for custom reports

You can generate custom reports by using the shared access objects in IBM Security Identity Manager. Use the shared access entities, such as credential, credential pool, credential lease, and shared access policy to generate the custom reports.

For more information about shared access entities and their corresponding attributes, see *Database and Directory Server Schema Reference* > *Database tables reference* > *Shared access tables* in the *IBM Security Identity Manager* product documentation.

Example: Creating custom report to view all shared access credentials checked out:

This topic provides detailed instructions to create custom reports to view all the shared access credentials that are currently checked out with examples.

Before you begin

Run the data synchronization process before you create a custom report to view all the shared credentials that are currently checked out. See "Data synchronization for reports" on page 337.

Procedure

To create a custom report to view all the shared access credentials that are currently checked out, complete these steps:

1. From the left navigation pane, select **Reports** > **Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.

8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

   Important: You must add at least one column to create the report.
10. Complete the following steps on this page:
    a. From the **Entity** and **Attribute** lists, select appropriate options. For example, to create a custom report for viewing all the credentials that are checked out, you can map the following entities and attributes.

Table 74. Entities and Attributes

Entity	Attribute	Mapping displayed on the Contents page
Credential	Name	Credential.Name
Credential lease	Credential Checkout Expiration Time	Credential lease.Credential Checkout Expiration Time
Credential lease	Credential Checkout Time	Credential lease.Credential Checkout Time

    Note: You can select the entities and attributes based on your requirements.
    b. In the **Column width** field, type the size of the column. The default value is 5.
    c. Click **OK** to add the column in the report.
11. Click the **Filter** tab to specify the data that must be displayed in the report. To do so, apply the filter conditions in the **Add a New Filter Row** area:
    a. Add rows with these filter conditions. Click **Add Row** after you finish adding every row.

Table 75. Filter conditions

Row	Entity	Attribute	Operator	Entity	Attribute	Condition
1	Credential	Name	Like	_USERINPUT_	-	AND
2	Credential	Service name	Like	_USERINPUT_	-	AND
3	Credential lease	Credential DN	Equals	Credential	DN	AND
4	Credential lease	Credential Lessee	Equals	Person	DN	AND
5	Service	Service Name	Like	_USERINPUT_	-	NONE

    Note: You can apply filter conditions based on your requirements. For information about entities, attributes, operators, and conditions, see the Security Identity Manager online help for the Filter page.
    b. Optional: Click **Preview** to open a new browser window that contains a preview of the report.
    c. Click **OK** after you apply all the filter conditions.
12. On the Success page, in the **Other Tasks** area, click **Run Custom Report**.
13. On the Options page, click the report whose data you want to view.
14. Optional: If you selected the **_USERINPUT_** entity in the filters that you specified earlier, narrow down the search scope of the report. For example:

a. In the **Credential Name Like** field, specify * to show all the credential names.
b. In the **Service Service Name Like** field, specify `Win*` to show all the services whose service name begins with *Win*.

15. Select the format of the report. You can select either PDF or CSV format.
16. Click **OK** to generate the report.

Results

A report is generated in a new window that shows all the shared access credentials that are currently checked out.

Example: Creating check in audit report:

This topic provides detailed instructions to create a report that displays audit information for the checked in credentials.

Before you begin

Run the data synchronization process before you create a check in audit report. See "Data synchronization for reports" on page 337.

Procedure

To create a report that displays audit information for the checked in credentials, complete these steps:

1. From the left navigation pane, select **Reports** > **Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

   Important: You must add at least one column to create the report.
10. Complete the following steps on this page:
    a. From the **Entity** and **Attribute** lists, select appropriate options. For example, to create a report that displays audit information for the checked in credentials, you can map the following entities and attributes.

Table 76. Entities and attributes

Entity	Attribute	Mapping displayed on the Contents page
Audit Event	Entity Name	Audit Event.Entity Name
Audit Event	Initiator Name	Audit Event.Initiator Name

Table 76. Entities and attributes (continued)

Entity	Attribute	Mapping displayed on the Contents page
Audit Event	Timestamp	Audit Event.Timestamp

Note: You can select the entities and attributes based on your requirements.

b. In the **Column width** field, type the size of the column. The default value is 5.

c. Click **OK** to add the column in the report.

11. Click the **Filter** tab to specify the data that must be displayed in the report. To do so, apply the filter conditions in the **Add a New Filter Row** area:

    a. Add rows with these filter conditions. Click **Add Row** after you finish adding every row.

Table 77. Filter conditions

Row	Entity	Attribute	Operator	Entity	Attribute	Condition
1	Audit Event	Action	Like	_USERINPUT_	-	AND
2	Audit Event	Entity Name	Like	_USERINPUT_	-	AND
3	Audit Event	Initiator Name	Like	_USERINPUT_	-	AND
4	Audit Event	Timestamp	Like	_USERINPUT_	-	NONE

Note: You can apply filter conditions based on your requirements. For information about entities, attributes, operators, and conditions, see the Security Identity Manager online help for the Filter page.

b. Optional: Click **Preview** to open a new browser window that contains a preview of the report.

c. Click **OK** after you apply all the filter conditions.

12. On the Success page, in the **Other Tasks** area, click **Run Custom Report**.
13. On the Options page, click the report whose data you want to view.
14. Optional: If you selected the **_USERINPUT_** entity in the filters that you specified earlier, narrow down the search scope of the report. For example,

    a. In the **Audit Event Action Like** field, select **Check in** from the list to view audit information for the checked in credentials.

    b. In the **Audit Event Entity Name Like** field, specify * to show all the entity names.

    c. In the **Audit Event Initiator Name Like** field, specify * to show all the initiator names.

    d. In the **Audit Event Timestamp Like** field, specify the date for which you want to view the audit information for the checked in credentials.

15. Select the format of the report. You can select either PDF or CSV format.
16. Click **OK** to generate the report.

Results

A report is generated in a new window that shows audit information for the checked in credentials.

Example: Creating role and shared access entitlement report:

This topic provides detailed instructions to create role and shared access entitlement report by using examples. The report provides you information about roles and groups by using which the entitlement is defined and other entitlement details.

Before you begin

Run the data synchronization process before you create role and shared access entitlement report. See "Data synchronization for reports" on page 337.

Procedure

To create role and shared access entitlement report, complete these steps:

1. From the left navigation pane, select **Reports** > **Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

   Important: You must add at least one column to create the report.
10. Complete the following steps on this page:
    a. From the **Entity** and **Attribute** lists, select appropriate options. For example, to create role and shared access entitlement report, you can map the following entities and attributes.

Table 78. Entities and attributes

Entity	Attribute	Mapping displayed on the Contents page
Group	Group ID	Group.Group ID
Organizational Container	Name	Organizational Container.Name
Organizational Role	Name	Organizational Role.Name
Shared Access Policy Entitlement View	Entitlement Name	Shared Access Policy Entitlement View.Entitlement Name
Shared Access Policy Entitlement View	Entitlement Service Name	Shared Access Policy Entitlement View.Entitlement Service Name
Shared Access Policy Entitlement View	Entitlement Target Name	Shared Access Policy Entitlement View.Entitlement Target Name

Table 78. Entities and attributes (continued)

Entity	Attribute	Mapping displayed on the Contents page
Shared Access Policy Entitlement View	Entitlement Type	Shared Access Policy Entitlement View.Entitlement Type

Note: You can select the entities and attributes based on your requirements.

b. In the **Column width** field, type the size of the column. The default value is 5.

c. Click **OK** to add the column in the report.

11. Click the **Filter** tab to specify the data that must be displayed in the report. To do so, apply the filter conditions in the **Add a New Filter Row** area:

a. Add rows with these filter conditions. Click **Add Row** after you finish adding every row.

Table 79. Filter conditions

Row	Entity	Attribute	Operator	Entity	Attribute	Condition
1	Shared Access Policy Entitlement View	Shared Access Policy DN	Equals	Shared Access Policy	DN	AND
2	Shared Access Policy	Parent DN	Equals	Organizational Container	DN	AND
3	Shared Access Policy Entitlement View	Entitlement Target DN	Equals	Credential Pool	DN	AND
4	Credential Pool	Groups	Equals	Group	DN	AND
5	Organizational Role	Name	Like	_USERINPUT_	-	NONE

Note: You can apply filter conditions based on your requirements. For information about entities, attributes, operators, and conditions, see the Security Identity Manager online help for the Filter page.

b. Optional: Click **Preview** to open a new browser window that contains a preview of the report.

c. Click **OK** after you apply all the filter conditions.

12. On the Success page, under the **Other Tasks** area, click **Run Custom Report**.
13. On the Options page, click the report whose data you want to view.
14. Optional: If you selected the **_USERINPUT_** entity in the filters that you specified earlier, narrow down the search scope of the report. For example, in the **Organization Role Name Like** field, specify * to show all the organizational roles.
15. Select the format of the report. You can select either PDF or CSV format.
16. Click **OK** to generate the report.

Results

A report is generated in a new window that shows role and shared access entitlement details.

Creating role custom report templates

Use the IBM Security Identity Manager report designer to create role custom report templates by using the role assignment attributes.

Before you begin

Run the data synchronization process before you create a custom report template. See "Data synchronization for reports" on page 337.

Procedure

To create a role custom report template, complete these steps:

1. From the left navigation pane, select **Reports** > **Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

   Important: You must add at least one column to create the report.
10. Complete the following steps on this page:
    a. From the **Entity** list, select an appropriate option. For example, select **Role Assignment Attributes**.
    b. From the **Attribute** list, select one of the options for adding it as a column in the report. For example, select **Attribute Name**.

       Note: Attribute list options are mapped with the entity that you selected earlier.
    c. In the **Column width** field, type the size of the column. The default value is 5.
    d. Click **OK** to add the column in the report.
11. Click the **Filter** tab, and then add or remove rows and columns for the report according to your requirements. For example, you can add a row in the report for a list of roles that have assignment attributes. To do so, complete these steps under the **Add a New Filter Row** area:
    a. From the **Entity** list, select **Organizational Role**.
    b. From the **Attribute** list, select **DN**.
    c. From the **Operator** list, select **Equals**.

d. From the **Entity** list, select **Role Assignment Attributes**.
e. From the **Attribute** list, select **Role Distinguished Name**.
f. From the **Condition** list, select one of these options:
   - None: Indicates that no more filter condition can be added to the report.
   - AND: Generates results only if all the specified filter conditions meet.
   - OR: Generates results if either of the specified filter conditions meet.

12. Optional: Click **Preview** to open a new browser window that contains a preview of the report.
13. Click **OK** to create the role custom report.

Results

A message is displayed, which indicates that you created the role custom report template.

What to do next

Generate the role custom report that you created either in a PDF or a CSV format. See "Generating custom reports" on page 317.

Report schema mapping

A *report schema* specifies which entities and attributes can be included in reports. Before an entity and its associated attributes can be specified as reporting criteria and included in custom report data, a report schema must be defined.

Schemas are installed for all of the standard reports during product installation. The administrator does not define schemas for standard reports.

By default, entities and attributes are not included in custom reports. The administrator must define a schema for each custom report template that is created, including designer reports. To create a report schema, you must run the Design Schema task in the console.

Note: Map only the entities and attributes for which you want to generate custom reports. These mappings directly affect the performance of IBM Security Identity Manager. The impact occurs because all of the data from the directory server is copied to the database each time a data synchronization is done.

By defining the schema, you select directory entities that are staged as tables in the IBM Security Identity Managers database. Defining the schema involves mapping attributes. After mapping the entities and attributes, you must synchronize the data to make the data available for reporting.

Mapping attributes:

To create a custom report schema, create an attribute mapping that specifies the entities and entity attributes that can be included in a report.

Before you begin

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

About this task

The type of data that can be included in a custom report is determined by the report schema. You do not create report schemas for standard reports because those schemas are already defined. The attributes for a particular entity can be unmapped if all the reports with that entity and attribute are deleted.

To map the attributes for an entity, complete these steps:

Procedure

1. Click **Report** > **Schema Mapping**. The Select Entity Attributes page is displayed.
2. On the Select Entity Attributes page, select an entity from the list of objects. Both mapped and unmapped attributes for the selected entity are displayed. If they are being used by standard reports, some of the attributes can be mapped by default.
3. Select one or more attributes from the **Unmapped attributes** list, and then click **Add**.
   - To select multiple attributes at the same time, press the Ctrl key and click each attribute that you want to map.
   - To select continuous, multiple attributes at the same time, press the Shift key and click each attribute that you want to map.

   The attribute is moved to the **Mapped attributes** list.
4. Click **OK** to save the report schema and close the Select Entity Attributes page.

Results

A message is displayed, indicating that you successfully updated the schema mapping for the entity that you selected.

What to do next

Select another reporting task, or click **Close**.

Unmapping attributes:

You can unmap previously mapped attributes so that they are no longer available for reporting.

Before you begin

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

About this task

Only attributes that are not being used in any reports can be unmapped. The attributes that you unmap are made unavailable for reporting as soon as you save your changes. You do not have to run the data synchronization task for the changes to take effect.

To unmap the attributes for an entity, complete these steps:

Procedure

1. Click **Report** > **Schema Mapping**. The Select Entity Attributes page is displayed.
2. On the Select Entity Attributes page, select an entity from the list of objects. Both mapped and unmapped attributes for the selected entity are displayed. If they are being used by standard reports, some of the attributes can be mapped by default.
3. Select one or more attributes from the **Mapped attributes** list, and then click **Remove**.
   - To select multiple attributes at the same time, press the Ctrl key and click each attribute that you want to unmap.
   - To select continuous, multiple attributes at the same time, press the Shift key and click each attribute that you want to unmap.

   The attribute is moved to the **Unmapped attributes** list.
4. Click **OK** to save the report schema and close the Select Entity Attributes page.

Results

A message is displayed, indicating that you successfully updated the schema mapping for the entity that you selected.

What to do next

Select another reporting task, or click **Close**.

User input values

Determine which user input values to specify when you run standard reports.

User input values describe:

- Fields in standard reports for which you can specify values when you run the reports.
- Types of values that you can specify for each field.
- Default values used for each field if you do not specify a value.

Table 80. User input values

Report field name	Values that can be specified	Default value used if no input is specified
Access Name	Name of an access or a string expression that contains one or more wildcards	Any
Access Type	Access type from list	Any
Account Operation	Any of the values displayed in the list	Any
ACI Context	Name of an entity type or the value "any," which is specified with the asterisk (*)	*, indicating any value
ACI Name	Name of a policy or a sting expression that contains one or more wildcards	*, indicating any value
ACI Object Type	Name of an object associated with the entity type, or the value "any"	Any

Table 80. User input values (continued)

Report field name	Values that can be specified	Default value used if no input is specified
ACI Scope	Any, single, or sub tree	Any, single, sub tree
Approval Activity	Name of an activity or a sting expression that contains one or more wildcards	*, indicating any value
Approver	Person (A person search is started to get a value.)	Any
Approver (Pending Approvals)	Person	Any
Organization Unit	Business unit	Any
Dormant Period	Integer	14 (days)
End date	Date in the format set for your locality	Current® date and time
Operations	Any of the values displayed in the list	Any
Person	Person	Any
Person - Suspended before	Date in the format set for your locality	Current date and time
Provisioning Policy Name	Name of a policy or a sting expression that contains one or more wildcards	*, indicating any value
Recertification Policy Target Type	Recertification policy target type from list	Any
Recertification Response	Recertification response type from list	Any
Requestee	Person	Any. For nonadministrative users, the default value is the owner of a user that is logged on.
Role	Role	Any
Root Process	Any of the values displayed in the list	Any
Service	Service	Any
Service owner	Person	Any
Service Type	Service type from the list	Any
Start Date	Date in the format set for your locality	30 days before current date and time
Status (Account)	Any, Active, or Inactive	Any
Status (Account Operation)	Any, Success, Warning, Failure, or Pending	Any
Status (Pending Approvals)	Any, Escalated, or Locked	Any
Submitted by	Person	Any
Suspended Before (Accounts and Individuals)	Date in the format set for your locality	Current date and time
User ID	Specific user ID or a sting expression that contains one or more wildcards	*, indicating any user ID

User input filters

Determine which filters to specify when you design custom reports that allow user input.

User input filters include:

- User input filters that you can specify for each type of standard report.
- Corresponding filter that is defined in each report template to enable user input for built-in designer reports.

Use the filters as guidelines to create user input filters for custom reports.

You can specify one or more filter values for a single report, depending on which user input filters are available for the report. If you specify multiple values, IBM Security Identity Manager determines the *entity.attribute* to which each value applies by the position and type of each value. For example, when you run an account report, you can specify a service name and an organization unit name in a field, such as **Provide User Input**.

Table 81. User input filters

Report name	User input	Default value	Report designer filter
Access Control Item	ACI Name	Any	`ACI.name = _USERINPUT_`
	ACI Context	Any	`ACI.category = _USERINPUT_`
	Object Type	Any	`ACI.Target = _USERINPUT_`
	ACI Scope	Any	`ACI.scope = _USERINPUT_`
	Organization Unit	Any	`Organizational Container.DN = _USERINPUT_`
Access Report	Access Type	Any	`Access.Type = _USERINPUT_`
	Access	Any	`Access.DN = _USERINPUT_`
	Service Type	Any	`Service.servicetype = _USERINPUT_`
	Service	Any	`Service.DN = _USERINPUT_`
	Owner	Any	`Person.DN = _USERINPUT_`
Account	Service	Any	`Service.DN = _USERINPUT_`
	Organization Unit	Any	`Organizational Container.DN = _USERINPUT_`
Account/Access Pending Recertification Report	Account/Access Owner	Any	`Process.Requestee = _USERINPUT_`
	Service Type	Any	`Service.Servicetype = _USERINPUT_`
Account Operations	Root Process	Any	`Process.Type = _USERINPUT_`
	Account Operation	Any	`Activity.Type = _USERINPUT_`
	Start Date	30 days before current date	`Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_`
	End Date	Current date	
	Service Type	Any	`Service.servicetype = _USERINPUT_`
	Service	Any	`Service.DN = _USERINPUT_`
	User ID	Any	`Activity.Subject = _USERINPUT_`
	Status	Any	`Activity.Result_ Summary = _USERINPUT_ (Any)`

Table 81. User input filters (continued)

Report name	User input	Default value	Report designer filter
Account Operations Performed by an Individual	Submitted by	Any	`Process.REQUESTER = _USERINPUT_`
	Account Operation	Any	`Activity.Type = USERINPUT_`
	Start Date	30 days before current date	`Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_`
	End Date	Current date	
	Service Type	Any	`Service.servicetype = _USERINPUT_`
	Service	Any	`Service.DN = _USERINPUT_`
	User ID	*	`Activity.Subject = _USERINPUT_`
	Status	Any	`Activity.Result_ Summary = _USERINPUT_`
Approvals and Rejections	Approver	Any	`Person.DN like _USERINPUT_ AND PERSON.CN = PROCESSLOG.REQUESTOR`
	Start Date	30 days before current date	`Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_`
	End Date	Current date	
	Service Type	Any	`Service.servicetype = _USERINPUT_`
	Service	Any	`Service.DN = _USERINPUT_`
	User ID	*	`Process.Subject = _USERINPUT_`
	Status	*	`PROCESS.RESULT_ SUMMARY like _USERINPUT_`
	Approval Activity		`ACTIVITY. DEFINITION_ID like _USERINPUT_`
Dormant Accounts	Service	Any	`Service.DN = _USERINPUT_`
	Dormant Period	14	`Last Accessed Date = _USERINPUT_`
Individual Access	Account Owner	Any	`Person.DN =_USERINPUT_`
	Organization Unit	Any	`OrganizationalContainer.DN =_USERINPUT`
	Access	Any	`Access.DN =_USERINPUT_`
	Service	Any	`Service.DN =_USERINPUT_`
Individual Accounts	Person	Any	`Person.DN = _USERINPUT_`
	Organization Unit	Any	`OrganizationalContainer.DN = _USERINPUT_`
Individual Accounts by Role	Role	None (no role specified)	`Organization Role.DN = _USERINPUT_`
	Organization Unit	Any	`OrganizationalContainer.DN = _USERINPUT_`
Non-Compliant Accounts	Service	Any	`Service.DN = _USERINPUT_`
	Reason	Any	`Account.eraccountcompliance = _USERINPUT_`
Operation	Requester	Any	`Process.REQUESTER = _USERINPUT_`
	Requestee	Any	`Process.REQUESTEE = _USERINPUT_`
	Operations	AccountAdd (as specified in the properties file)	`Process.Type = _USERINPUT`
	Start Date	30 days before the current date	`Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_`
	End Date	Current date	

Table 81. User input filters (continued)

Report name	User input	Default value	Report designer filter
Orphan Accounts	Service	Any	`Service.DN = _USERINPUT_`
	Account Status	Any	`Account.eraccountstatus = _USERINPUT_`
Pending Approvals	Approver	Any	`Person.DN = _USERINPUT_`
	Start Date	30 days before current date	`Workitem.Created > _USERINPUT_ AND Workitem.Created < _USERINPUT_`
	Service Type	Any	`Service.Servicetype = _USERINPUT_`
	Service	Any	`Service.DN = _USERINPUT_`
	User ID	*	`Process.Subject = _USERINPUT_`
	Status	Any	`Pending_Approval. Result_Summary = _USERINPUT_`
	Approval Activity Name	*	`Activity.Name = _USERINPUT_`
Policies Governing a Role	Role	Any	`Organization Role.DN = _USERINPUT_`
Policy	Provisioning Policy Name	Any	`ProvisioningPolicy. Policy Name = _USERINPUT_`
Recertification Change History Report	Service	Any	`Recertificationlog. Service = _USERINPUT_`
	Access Type	Any	`Recertificationlog. Access_Type = _USERINPUT_`
	Account/Access Owner	Any	`Recertificationlog. Account_Owner = _USERINPUT_`
	Recertification Response	Any	`Recertificationlog. Recert_Result = _USERINPUT_`
	Show Last Recertification Only	Yes/No	
	Start Date	30 days before current date	`Recertificationlog. Completed > _USERINPUT_ AND Recertificationlog. Completed < _USERINPUT`
	End Date	Current date	
Recertification Policy Report	Recertification Policy Target Type	Any	`RecertificationPolicy. GROUPDN LIKE '_USERINPUT_'`
	Service Type	Any	`RecertificationPolicy. SERVICETYPE = _USERINPUT_`
	Service	Any	`RecertificationPolicy. SERVICEDN =_ USERINPUT_`
	Access Type	Any	`RecertificationPolicy. ACCESSTYPE = _USERINPUT_`
	Access	Any	`RecertificationPolicy. ACCESSDN = _USERINPUT_`
Reconciliation Statistics	Service	None (input required)	`Service.DN = _USERINPUT_`
Rejected	Requester	Any	`Process.REQUESTER = _USERINPUT_ (Any)`
	Requestee	Any	`Process.REQUESTEE = _USERINPUT_ (Any)`
	Start Date	30 days before the current date	`Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_`
	End Date	Current date	

Table 81. User input filters (continued)

Report name	User input	Default value	Report designer filter
Services	Service Type	Any	`Service.servicetype = _USERINPUT_`
	Service	Any	`Service.DN = _USERINPUT_`
	Owner	Any	`Person.DN = _USERINPUT_`
	Organization Unit	Any	`Organizational Container.DN = _USERINPUT_`
Services Granted to an Individual	Person	Any	`Person.DN = _USERINPUT_`
Summary of Accounts on Service	Service	Any	`Service.DN = _USERINPUT_`
	Account Status	Any (as specified in the properties file)	`Account.Account Status = _USERINPUT_`
Suspended Accounts	Account	Any	`Account.DN = _USERINPUT_`
	Person	Any	`Person.DN = _USERINPUT_`
	Service Type	Any	`Service.servicetype = _USERINPUT_`
	Service	Any	`Service.DN = _USERINPUT_`
	Suspended Date	Current date	`Process.Completed < _USERINPUT_`
Suspended Individuals	Person	Any	`Person.DN = _USERINPUT_`
	Organization Unit	Any	`Organizational Container.DN = _USERINPUT_`
	Suspended Before	Current date	`Process.Completed < _USERINPUT_`
User	Requester	Any	`Process.REQUESTER = _USERINPUT_ (Any)`
	Requestee	Any	`Process.REQUESTEE = _USERINPUT_ (Any)`
	Start Date	30 days before the current date	`Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_`
	End Date	Current date	

Filter conditions for custom reports

Filter conditions are logical expressions that are parsed as a JOIN condition to determine what information to include in a report when it is generated.

You can create a simple filter condition with one operator:

```
Account.Service Equals Service.DN
```

You can also create complex filters with multiple conditions:

```
ACI.DN = ACI Principals.DN
AND ACI.Name = ACI Principals.Name
AND ACI.Target = ACI Principals.Target
```

Example: Creating filter conditions for accounts:

This example report lists users with accounts of type `ITIMService`.

Assume that you specified the following entities, attributes, and filters to create the report template:

- **Report columns:** Account.Userid, ITIM.ServiceName
- **Filters:** None

Because no JOIN filter is specified, if there are two users:

- User1 with ITIMService1 and ITIMService2
- User2 with ITIMService3

The result is:

User1	ITIMService1
User1	ITIMService2
User1	ITIMService3
User2	ITIMService1
User2	ITIMService2
User2	ITIMService3

This result is the Cartesian product of the two tables; it does not display the wanted results. To yield the appropriate result set, specify the appropriate JOIN condition to indicate the relationships between these two tables. The JOIN condition in this case is:

```
Account.Service = ITIM.DN
```

If you specify this filter, the result is:

User1	ITIMService1
User1	ITIMService2
User2	ITIMService3

Example: Creating filter conditions for persons and organization roles:

This report shows persons associated with an organization role.

Assume that you specified the following entities, attributes, and filters in the console to create the report template:

- **Report columns:** Person.FullName, OrganizationRole.Name
- **Filter:** OrganizationRole.Name = '_USERINPUT_'

Assume that there are two users:

- Person1 with Role1
- Person2 with Role2

If you enter `Role1` as user input when you run the report, the result is:

Person1	Role1
Person2	Role1

For this report to generate the correct results, specify the following filter:

```
Person.OrganizationRoles = OrganizationRole.DN
AND OrganizationRole.Name = '_USERINPUT_'
```

Now, if you enter `Role1` as user input when you run the report, the result would be:

Person1	Role1

The specified filter condition works because the Organization Roles attribute of the Person contains the value of the DN of the role to which a user belongs. Also note that Organization Role is a multi-valued attribute; that is, a person can have multiple roles in an organization.

Example: Creating filter conditions for persons and accounts:

This report shows accounts associated with persons defined to IBM Security Identity Manager.

Assume that you specified the following entities, attributes, and filters in the console to create the report template:

- **Report column:** Person.FullName, Account.AccountStatus
- **Filters:** None

This report returns the Cartesian product of the Person and Account table entries. To yield the correct result, the JOIN condition that specifies the relationship between the Person and Account tables is:

```
Account.owner = Person.DN
```

Sample JOIN conditions for designing reports:

Review examples of filters that you can use to design custom reports.

The Filters column contains the exact JOIN condition that yields accurate and meaningful results.

Note: The Serial No. column is included only for referencing by support personnel.

Serial No.	Entities	Filters
1	Person, Account	`Person.DN = Account.owner`
2	Person, Organization Role	`Person.Organization Roles = Organization Role.DN`

3	Person, Organizational Unit	`Person.ParentDN = Organizational Unit.DN`
		`OR`
		`Organizational Unit. Supervisor = Person.DN`

4	Account, Service	`Account.Service = Service.DN`
5	Location, Person	`Location.Supervisor = Person.DN`
6	Business Partner, Organization, Person	`Business Partner Organization.Sponsor = Person.DN`
7	Business Partner Person, Organization Role	`Business Partner Person.Organization Roles = Organization Role.DN`
8	Organization, Location	`Organization.DN = Location.Parent DN`

9	Organization, Organizational Unit Organization, Business Partner Organization	Organization.DN = Organizational Unit.ParentDN Organization.DN = Business Partner Organization.ParentDN
10	Organizational Unit, Location	Organizational Unit.Parent DN = Location.DN OR Location.Parent DN = Organizational Unit.DN
11	Organizational Unit, Business Partner Organization	Organizational Unit.Parent DN = Business Partner Organization DN OR Business Partner Organization.Parent DN = Organizational Unit.DN
12	Location, Business Partner Organization	Location.Parent DN = Business Partner Organization.DN OR Business Partner Organization.Parent DN = Location.DN
13	Service, Person	Service.Account Owner = Person.DN
14	SQL2000Account, Service	SQL2000Account.Service = Service.DN
15	ITIMAccount, ITIM Service	ITIMAccount.Service = ITIM.DN
16	Entitlement, Service	Service.DN = Entitlement.Service Target Name
17	Provisioning Policy, Entitlement	ProvisioningPolicy.DN = Entitlement.DN
18	ACI, ACI Principals	ACI.DN = ACI Principals.DN AND ACI.Name = ACI Principals.Name AND ACI.Target = ACI Principals.Target
19	ACI, ACI Permission ClassRight	ACI.DN = ACI Permission ClassRight.DN AND ACI.Name = ACI Permission ClassRight.Name AND ACI.Target = ACI Permission ClassRight.Target
20	ACI, ACI Permission AttributeRight	ACI.DN = ACI Permission AttributeRight.DN AND ACI.Name = ACI Permission AttributeRight.Name AND ACI.Target = ACI Permission AttributeRight.Target
21	ACI, ACI Role DNs	ACI.DN = ACI Role DNs.DN AND ACI.Name = ACI Role DNs.Name AND ACI.Target = ACI Role DNs.Target
22	ACI, Organizational Unit	ACI.DN = Organizational Unit.DN

Customizing the report banner

You can add a customized banner to your IBM Security Identity Manager reports.

Before you begin

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

About this task

Use this task to produce reports that display the logo of your organization in the header.

To add a customized banner, complete these tasks:

Procedure

1. Create your custom banner as a Graphic Interchange Format (GIF) file, with `logo.gif` as the file name.
2. Place the `logo.gif` file in the *ISIM_HOME*`/data/adhocreport/logo` directory.
3. Ensure that the `logo.gif` file provides read permission that allows the web application server to access the file.
4. To validate that the customized banner is used, generate and view a report. If the customized banner is not displayed, restart your browser.

Custom report configuration files

You can modify properties files to change settings that are related to custom reports and to add user-defined functions to the custom reports tasks.

adhocreporting.properties
This file contains configuration properties related to the custom reporting tasks.

DatabaseFunctions.conf
You can specify user-defined database functions when designing custom report templates. For example, to retrieve an attribute from a table column in the staged data, IBM Security Identity Manager provides two functions, upper and lower. Use these functions to specify that the data is returned for display in uppercase or lowercase letters. To make available user-defined functions, add the functions to this file.

Data synchronization

IBM Security Identity Manager stores most of its operational data in an LDAP directory. Examples of operational data include information about the people and accounts that are managed by IBM Security Identity Manager, the policies that are defined in IBM Security Identity Manager, and other information.

IBM Security Identity Manager provides the ability for users to run reports about this operational data. For example:

- As an auditor, you might want to run a report that lists all of the people who are in violation of a corporate policy.
- As an administrator, you might want to run a report that lists all of the accounts that are inactive for the last six months.
- As a manager, you might want to run a report that lists all of the accounts that are owned by people in your department.

The reporting architecture requires that data reside in a database. The IBM Security Identity Manager data synchronization feature copies the operational data from the LDAP directory to a database, making it available to be included in reports.

Running data synchronization

Data synchronization can be run in the following ways:

Full data synchronization

This approach synchronizes all of the operational data. That is, the full data synchronization process starts by deleting all of the data it previously copied into the database. Then, it copies all of the operational data from the LDAP directory to the database. The full data synchronization can be run in the following ways:

On demand

As an administrator, you can log in to IBM Security Identity Manager, and run the full data synchronization process.

On a recurring schedule

As an administrator, you can configure IBM Security Identity Manager to automatically run the full data synchronization process on a specified recurring schedule. For example, you can configure IBM Security Identity Manager to run the full data synchronization process at these times:

- Every Sunday night at midnight.
- The 15th day of every month.

Incremental data synchronization

This approach synchronizes only the operational data that changed since the last time the data was synchronized. Unlike the full data synchronization, the incremental data synchronization does not delete all of the data it previously copied into the database. Rather, it updates the database to reflect the changes that occurred in the LDAP directory since the last time the data was synchronized. Incremental data synchronization requires enabling the LDAP change log feature.

Report Data Synchronization Utility

This approach is identical to the full data synchronization. The only difference is that it can be run from a computer that is not part of the deployed IBM Security Identity Manager environment. That is, the first two approaches must be run on a computer in which IBM Security Identity Manager is installed. The Report Data Synchronization Utility can be run on any computer, provided the computer meets the hardware and software requirements of the utility.

Data synchronization for reports

Manage schedules for data synchronization, or initiate a data synchronization activity immediately. You can also refresh the synchronization status.

When you initiate a data synchronization activity, the following actions occur:

- Directory server data is staged for report processing
- Mapping updates that are made with the Schema Mapping task are made available to the Design Report task
- Data and ACI information is synchronized between the directory server and the database
- All separation of duty policies defined in the system are evaluated for violations

Data synchronization schedules that you add are run as a background process at the scheduled time.

In general, schedule the data synchronization task when system load is low.

You can initiate a data synchronization activity immediately, or you can schedule a task to run at a specified time or at regular intervals.

You can view the status of the most recent data synchronization.

You can add or modify data synchronization schedules at any time.

You do not need to do a data synchronization task when you modify a report. However, if you change the report schema, reporting ACIs, or the entity data, you must do a data synchronization for the changes to take effect. For example, you might add a person to the system and want the name of that person to occur in a report.

The entities and attributes that you map with the Schema Mapping task are made available for the Design Report task only after data is synchronized.

Synchronizing data immediately

You can initiate an immediate data synchronization activity.

Before you begin

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

About this task

To initiate a data synchronization activity immediately, complete these steps:

Procedure

1. Click **Reports** > **Data Synchronization**.
2. On the Data Synchronization page, click **Run Synchronization Now**. A confirmation page is displayed.
3. On the Confirm page, click **Run Synchronization Now** to run the synchronization, or click **Cancel**.

Results

A message is displayed, indicating that you successfully initiated a data synchronization activity.

What to do next

To view the results of the synchronization, click **Return to the Data Synchronization page**. You can also select another reporting task, or click **Close**.

Creating a data synchronization schedule

You can create a schedule for synchronizing data.

Before you begin

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

About this task

To create a data synchronization schedule, complete these steps:

Procedure

1. Click **Reports** > **Data Synchronization**.
2. On the Data Synchronization page, click **Create**. The Synchronization Schedule page is displayed.
3. Select a schedule interval to synchronize data on the system. The fields displayed depend on the scheduling option that you select.
4. Complete any remaining fields as wanted, and then click **OK** to save the new schedule.

Results

A message is displayed, indicating that you successfully added the new synchronization schedule.

What to do next

Select another reporting task, or click **Close**.

Modifying a data synchronization schedule

You can modify an existing schedule for synchronizing data.

Before you begin

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

A data synchronization schedule must exist.

About this task

To modify a data synchronization schedule, complete these steps:

Procedure

1. Click **Reports** > **Data Synchronization**.
2. On the Data Synchronization page, click the schedule that you want to modify. The Synchronization Schedule page is displayed.
3. Select a schedule interval to synchronize data on the system. The fields displayed depend on the scheduling option that you select.
4. Complete any remaining fields as wanted, and then click **OK** to save the modified schedule.

Results

A message is displayed, indicating that you successfully updated an existing synchronization schedule.

What to do next

Select another reporting task, or click **Close**.

Deleting a data synchronization schedule

You can delete one or more schedules for data synchronization.

Before you begin

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

A data synchronization schedule must exist.

About this task

To delete a data synchronization schedule, complete these steps:

Procedure

1. Click **Reports** > **Data Synchronization**.
2. On the Data Synchronization page, select the check box next to the synchronization schedule that you want to delete. Selecting the check box at the top of this column selects all synchronization schedules.
3. Click **Delete** A confirmation page is displayed.
4. On the Confirm page, click **Delete** to delete the selected synchronization schedule, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the synchronization schedule.

What to do next

Select another reporting task, or click **Close**.

Incremental data synchronizer overview

The Incremental Data Synchronizer is a separately installed utility that provides fast synchronization of data and access control items. Synchronization occurs between the directory server that IBM Security Identity Manager uses and the IBM Security Identity Manager database.

In addition, the Incremental Data Synchronizer can be configured to enforce changes in the schema entities and attribute mappings that are used in custom report templates.

The Incremental Data Synchronizer synchronizes staged reporting data (entities and attributes) and corresponding access control item information for the data. Additionally, it can propagate schema changes. The Incremental Data Synchronizer does the following operations:

1. Changelog synchronization:
   a. Obtain the changelogs from the directory server.
   b. Analyze the effective operation and attribute values of each modified entry.
   c. Update the access control item information, if necessary.
   d. Update all available entry attributes in the staged tables with the changes recorded in the directory changelog.

2. Schema enforcement:
   a. Determine any changes made to the report schema.
   b. Map or unmap entities, if necessary.
   c. Map or unmap entity attributes, if necessary.
   d. Add or remove the access control item information of the newly mapped and unmapped attributes.

A fully configured Incremental Data Synchronizer does the same functions as the built-in data synchronizer. However, it manages incremental changes to the data and does the synchronization task only on the changed data. By propagating only the changes since the last synchronization task was done, the Incremental Data Synchronizer can update the staged reporting data quickly.

You install and configure the Incremental Data Synchronizer after installing IBM Security Identity Manager. Incremental data synchronization is not a prerequisite for custom reports unless your environment requires a fast synchronization of data and access control item definitions.

The more often you run the Incremental Data Synchronizer, the less likely you are to have errors in the data. You are less likely to have errors in the access permissions to the report data. The accuracy of the custom reporting process is enhanced.

For information about the Incremental Data Synchronizer, search for **Incremental Data Synchronizer** in the IBM Security Identity Manager documentation.

Directory Server changelog

The Incremental Data Synchronizer uses a mechanism known as changelog, a feature provided by the directory server.

The changelog is a history of changes maintained by the directory. Directory servers supported by IBM Security Identity Manager can be configured to record data changes under a directory node called:

```
cn=changelog
```

The Incremental Data Synchronizer fetches change entries stored under the cn=changelog directory. The Incremental Data Synchronizer picks up the data and access control item change entries needed to synchronize with the staged database tables.

To enable changelog for the specific directory server used by IBM Security Identity Manager, see the appropriate documentation provided by the vendor of that directory server.

Note: Enabling the IBM Security Identity Manager Server changelog can reduce directory update performance by 10 to 15 percent.

Definitions for HOME and other directory variables

The table contains default definitions that represent the HOME directory level for different product installation paths.

Path Abbreviation	Description
ISIM_HOME	*INSTALL_DIR*/ISIM *INSTALL_DIR* is the location of the IBM Security Identity Manager Server installation.
WAS_HOME	*INSTALL_DIR*/WebSphere/AppServer/ *INSTALL_DIR* is the location of the WebSphere Application Server installation.
WAS_CLIENT_HOME	*WAS_CLIENT_HOME* is the location of the Application Client for WebSphere Application Server Version 6.1. For example, *WAS_CLIENT_HOME* might refer to D:\Program Files\IBM\WebSphere\AppClient on a Windows system.

Starting the incremental data synchronizer

Start the IBM Security Identity Manager Server and synchronize the data with the Synchronize Data task in the IBM Security Identity Manager console *before* you start the Incremental Data Synchronizer.

Before you begin

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

About this task

You can start the Incremental Data Synchronizer either in graphical user interface mode or in command-line mode. To access the graphical user interface when the Incremental Data Synchronizer is installed on a UNIX or Linux computer, from a remote Windows computer, you must first connect the Windows computer to the UNIX system with an appropriate X Server-based environment.

You can run the Incremental Data Synchronizer immediately or schedule its execution. However, *you must run the Incremental Data Synchronizer interactively the first time you use it.* During the initial session, you can specify the time intervals for running the utility in the future. You can set the changelog synchronization and schema enforcement features independently as required.

Starting the Incremental Data Synchronizer user interface:

You can use a graphical user interface to run the Incremental Data Synchronizer.

Before you begin

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

Install the Incremental Data Synchronizer.

Procedure

1. Start Incremental Data Synchronizer:

   From UNIX

- Use XClient to start the Incremental Data Synchronizer.
- To start the Incremental Data Synchronizer user interface in the WebSphere Application Server, run the following script in the *ISIM_HOME*/bin/unix directory:

  ```
  # startIncrementalSynchronizerUI_WAS.sh
  ```

From Windows

To start the Incremental Data Synchronizer user interface in the WebSphere Application Server, run the following script in the *ISIM_HOME*\bin\win directory:

```
startIncrementalSynchronizerUI_WAS.bat
```

2. To start access control item synchronization, you must first enter the credentials of the administrator for the IBM Security Identity Manager.
3. Click **Login** after you enter these credentials.
4. Enter the base DN in the LDAP directory server, where the *changelog* entries are stored and the time delay between two successive synchronizations. The time delay is the interval between the end of one synchronization and the start of the next synchronization.
5. To set these parameters, click **Options**.
6. Click **OK** to save the changes.
7. Click **Start** to start the synchronization. The progress of the synchronization and other details are shown in the text area of the graphical interface.
8. To stop the synchronization process, click **Stop**.
9. To clear the text area of the Incremental Data Synchronizer, click **Clear**.
10. Click **Exit** to exit from the Incremental Data Synchronizer.

Running a command to start the Incremental Data Synchronizer:

You can use a command to start the Incremental Data Synchronizer.

Before you begin

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

About this task

To start the Incremental Data Synchronizer with a command in WebSphere Application Server, you run a script, depending on your operating system. Optionally, you can run the Incremental Data Synchronizer in the background without any informational messages by specifying `runInBackground` as the last argument.

Procedure

1. Access the command-line interface.
2. Run one of the following scripts:

UNIX

Run the following script in the *ISIM_HOME*/bin/unix directory:

```
# startIncrementalSynchronizerCMD_WAS.sh itim-manager passwd
chglog-base-dn time-int
```

Windows

Run the following script in the *ISIM_HOME*\bin\win directory:

```
startIncrementalSynchronizerCMD_WAS.bat itim-manager passwd
chglog-base-dn time-int
```

Where:

Argument	Description
itim-manager	Login ID of IBM Security Identity Manager system administrator
passwd	Password for login ID
chglog-base-dn	Base DN of Security Identity Manager directory server *changelog* entries, for example, `cn=changelog`
time-int	Time interval between successive synchronizations
runInBackground	Runs the Incremental Data Synchronizer in the background without any informational messages.

3. To exit the Incremental Data Synchronizer, type system-specific interrupt characters, such as `Ctrl+C` on Windows systems.

Example

UNIX:

```
startIncrementalSynchronizerCMD_WAS.sh "itim manager" password "cn=changelog" 1800
```

Windows: entered as one line:

```
startIncrementalSynchronizerCMD_WAS.bat "itim manager" password
"cn=changelog" 1800
```

Fine-tuning the Incremental Data Synchronizer

You can tune the performance of the Incremental Data Synchronizer by modifying properties in the `adhocreporting.properties` configuration file.

The following three properties can be modified in combination to produce efficient operation of the synchronization process:

- **changeLogFetchSize**
- **maximumChangeLogsToSynchronize**
- **changeLogsToAnalyzeBeforeSynchronization**

For more information, see the *IBM Security Identity Manager Performance and Tuning Guide*.

Utility for external report data synchronization

The report data synchronization utility is a separately installed utility that synchronizes data and access control items between the directory server and the IBM Security Identity Manager database. The synchronized data is used for running the reports.

You can install, configure, and run the utility either on the same computer as IBM Security Identity Manager or on a different computer. If you install the utility on a different computer, that computer does not require the installation of the Application server, a directory server, or a database.

The utility for external report data synchronization is used for remote or non-IBM Security Identity Manager purposes. The IBM Security Identity Manager installer does not install the utility. You must manually install it by copying and extracting the `isim_report_data_sync_utility.zip` file from the `ISIM_HOME/bin` directory before using it.

Running the report data synchronization utility

After you configure the utility, you can start the synchronization process.

Before you begin

- Configure IBM Security Identity Manager report data synchronization utility.
- Access the folder in which you extracted the utility.

About this task

To run the report data synchronization utility, complete these steps:

Procedure

1. Run one of the following commands:

   Microsoft Windows platforms

   ```
   SyncData.cmd [-JAVA_HOME java_home_value]

   For example, SyncData.cmd -JAVA_HOME "C:\Program
   Files\IBM\Java60"
   ```

   UNIX or Linux platforms

   ```
   ./SyncData.sh [-JAVA_HOME java_home_value]

   For example, ./SyncData.sh -JAVA_HOME /opt/IBM/Java60
   ```

   where, `-JAVA_HOME` is an optional argument that specifies the location of the Java runtime environment. See Table 82 for specifying the location of the Java runtime environment.

Table 82. Specifying the location of the Java runtime environment

If the `-JAVA_HOME` argument is	IBM Security Identity Manager
• Specified	Uses the corresponding Java runtime environment.
• Not specified, and • The `-JAVA_HOME` operating system environment variable contains a value.	Uses the Java runtime environment corresponding to the `-JAVA_HOME` operating system environment variable.
• Not specified, and • The `-JAVA_HOME` operating system environment variable either does not exist or does not contain a value.	Reports a failure for the report data synchronization utility.

2. If you encounter any problem while running the report data synchronization utility, see the `SyncData.log` file. This log file is created in the directory where you extracted the utility.

What to do next

- See "Report data synchronization utility errors and their workarounds" on page 346.

Report data synchronization utility errors and their workarounds

The following topic describes how to troubleshoot the IBM Security Identity Manager report data synchronization utility errors.

The report data synchronization utility completes the data synchronization operation successfully, but with the following exception.

The following exception might get registered into the trace file:

```
Class com.ibm.websphere.cache.DistributedMap NOT FOUND
```

It might happen because the synchronization time exceeds the cache refresh timeout interval specified by the `enrole.profile.timeout` property. This exception does not affect the success of the data synchronization. You can ignore this exception message.

Workaround:

Increase the timeout interval value for the property `enrole.profile.timeout` in the `enRole.properties` property file.

The report data synchronization utility completes with a failure with log entries and indicates that the data synchronization cannot run because data synchronization is already running.

Follow the steps to end the data synchronization operation process and rerun the data synchronization utility. For more information about how to end the data synchronization operation, see http://www.ibm.com/support/docview.wss?uid=swg21303678.

The report data synchronization utility completes with a failure with log entries and indicates that the data synchronization failed with an `OutOfMemoryError` message.

`OutOfMemoryError` can occur if the Java virtual machine heap is too small.

Workaround:

Increase the Java virtual machine heap size by creating an operating system environment variable:

Microsoft Windows operating systems

```
set IBM_JAVA_OPTIONS=-Xms1024m -Xmx2048m
```

UNIX or Linux operating systems

```
export IBM_JAVA_OPTIONS='-Xms1024m -Xmx2048m'
```

where:

`-Xms1024m` specifies initial heap size of 1024 mb

`-Xmx2048m` specifies maximum heap size of 2048 mb

Note: The numbers mentioned in the instructions are examples only. The exact numbers that are required might vary.

Access control items (ACI) for reports

Access control item (ACI) definitions govern the availability of reports for all users. The report ACIs grant or deny a group of users the ability to run reports.

A IBM Security Identity Manager administrator can access all reports. In addition, there are default ACIs for the Manager, Service Owner, and Auditor groups. For example, service owners and managers can search for all persons that they can access. Managers can see direct reports, and service owners can see people on services controlled by ACIs. Auditors can run all reports and see all data. No report access is available for users or members of the Help Desk group, unless an

administrator creates an ACI definition that grants access to a group of which the user is a member. ACI definitions must be defined for both standard and custom reports.

An administrator can create an ACI definition at any time. After an ACI definition is added, the system immediately applies the ACI. The new ACI affect users who are logged in to the system and not currently viewing the list of available reports. Those users currently viewing the list of reports are not affected.

Users can view only activities that are specific to their group, either as submitters of the requests or as persons for whom the requests are submitted. For example, managers can view reports for requests that they initiated or for requests that are made for them. Employees that are not in supervisory or managerial roles can view only reports for requests that are made for them because they cannot initiate requests. Auditors can see requests generated by other users.

Report ACIs are applicable in only one organization. Therefore, for non-administrative users of secondary organizations to be able to run reports, report ACIs must also be created in those secondary organizations.

ACI object filters used for reporting

Object filters defined in ACIs are used by the reporting engine to stage data and ACI information in the database.

The reporting engine requires object filters that meet these conventions:

- The supported filters for LDAP to SQL conversion are a subset of filters mentioned in RFC 2254 for LDAP Filter Specification.
- Matching rules, soundex filters, and approximation operators are not supported.
- In regular expressions, only the * (asterisk) wildcard character is supported.
- Only the following special characters are allowed in LDAP filters:
  - $ (dollar sign)
  - @ (at sign)
  - _ (underscore)
  - * (asterisk)
  - ? (question mark)
  - / (forward slash)
  - \ (backward slash)
  - . (period)
  - : (colon)
  - space
  - tab
- The following characters are not supported in LDAP filters. If you use these characters in an object filter, the reporting engine does not consider the characters for ACI information staging:
  - { open curly brace
  - } close curly brace
  - [open box bracket
  -] close box bracket
  - % (percent sign)
  - & (ampersand)

  - , (comma)
- As specified within RFC 2254, these special characters can be used as normal characters in attribute values:
  - \2a to use * as a normal character, not as a wildcard
  - \28 to use (as a left parenthesis character
  - \29 to use) as a right parenthesis character
  - \5c to use \ as a backslash character

Chapter 11. Policy administration

For your organization, you can manage policies, which are sets of organizational rules and logic.

IBM Security Identity Manager supports the following types of policies:

- Adoption policies
- Identity policies
- Password policies
- Provisioning policies
- Recertification policies
- Separation of duty policies
- Service selection policies

Adoption policies

During reconciliation, an *adoption policy* determines the owner of an account. An account without any owner is an *orphan account*.

An adoption policy can apply to more than one service of the same service type. An adoption policy applies only to service types that represent adapters and manual services, not service types that represent identity feeds.

An adoption policy matches the attributes for an account on a managed resource to the attributes for a Security Identity Manager user.

An adoption policy applies to the following circumstances:

- To either the entire system, as a global adoption policy, or to a specific type of managed resource, as a service-specific adoption policy. The service-specific adoption policy takes precedence over the global adoption policy.
- To more than one service.
- Only to service types that represent adapters and manual services, not service types that represent identity feeds.

Note: You cannot define service instances of different types on the same adoption policy. Account ownership assigned by adoption policies is always of the `INDIVIDUAL` account ownership type.

JavaScript can define adoption policies. These policies use all standard JavaScript functions and programming constructs, such as loops and conditional branches. The policies also use functions that are designed specifically for creating adoption policies. Specific JavaScript functions that return a person can retrieve personal attribute values to evaluate account owners.

Global adoption policies are defined for a service type or all service types. Global adoption policies apply to all service instances if no adoption policy is defined for the specific service. The default global adoption policy assigns an account to a user if the account user ID attribute matches the Security Identity Manager user `UID` attribute.

Creating an adoption policy

An administrator can create an adoption policy to use when reconciling accounts for one or more services. For example, you might create a policy that determines account ownership by attempting to match the family name of a user with the account user ID.

Before you begin

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

Before you can create an adoption policy, you must create one or more services to associate with the policy. If you try to create an adoption policy with a service that is already the target of an adoption policy, an error message is displayed.

About this task

To create a global adoption policy (for a specific service type), you must navigate to **Configure System** > **Global Adoption policies**.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Adoption Policies**.
2. On the Work With Adoption Policies page, in the **Adoption Policies** table, click **Create**.
3. On the Manage Adoption Policies page, on the General page, type a name for your adoption policy.
4. Click the Services page, and then add one or more specific services to associate with the policy. To add one or more services:
   a. Click **Add**.
   b. On the Services page, type your search criteria, and then click **Search**.
   c. In the **Services** table, select one or more services.
   d. Click **OK**.
5. On the Manage Adoption Policies page, click the Rule page, and then specify the attributes that the adoption policy uses to match accounts to users.

   If you want to define matches, click **Add a match field** to select the account and user attributes that must match during reconciliation. The user attribute list provides a few common attribute combinations when defining the match. Such a combination might be the first letter of a given name plus the family name. The combination might be the given name plus the first letter of the family name. If your adoption policy is more complex, you can choose the more advanced path by selecting **Provide a Script**. If you defined matches, the associated scripts are populated for you in the script definition field.

   Important: If you want to provide a script, the IBM Security Identity Manager Server does not verify that the JavaScript is correct. Verify that the JavaScript is correctly coded before using it to define the adoption policy.
6. Click **OK** to save the changes.
7. On the Success page, click **Close**. On the Work With Adoption Policies page, you can search to see the new adoption policy displayed in the table. The table controls can be used to change or delete the policy.

JavaScript examples for writing adoption policies

An administrator of IBM Security Identity Manager, and can use JavaScript examples to write adoption policies.

Example 1

The following example shows a simple script that matches the account user ID to the alias field of the person.

```
var ps = new PersonSearch();
return ps.searchByFilter("","(eraliases="+subject.eruid[0]+")",2);
```

Example 2

This example is a more complicated sample you can use for orphan adoption. This script uses the following three strategies to deduce an owner for an account:

1. Locate a single person with an `eraliases` entry that matches the account **eruid** field.
2. If this action yields multiple matches and the new entry has a **cn** field, check the matching list for one with a **cn** field that matches the account **cn** field.
3. If no matches are obtained in the first step, check for a matching account (the same `eruid`) in the master service, such as a Windows Active Directory Service. If this account has an owner, use that person. If all three strategies fail, return null, which causes an orphan.

Note: Log messages are written to the message log with the script category.

```
var entryUid = subject.eruid[0];
Enrole.log("script", "Starting script for eruid=" + entryUid);
/* change the following value to the name of the master service: */
/* var masterServiceName = "Master AD Service";
*/
var masterServiceName = "NT4 (local)";
/* change the following value to the service profile name of the master service:
    This change is required only if the profile of master service and profile of the
    service for which the adoption policy is defined are different */
/* var serviceProfileNameOfMasterService = "ADProfile";
*/
var scriptResult = null;
var personsearch = new PersonSearch();
var filter = "(eraliases=" + entryUid + ")";
var psResult = personsearch.searchByFilter("", filter,2);
if (psResult.length == 1) {
 /* found one person with matching alias */
 Enrole.log("script", "single match for eraliases=" + entryUid);
 scriptResult = psResult;
}
else if (psResult.length > 1) {
 /* more than one person matched alias.
  * if the account has a "cn" attribute value, see if this matches
the "cn" of one of them
  */
 Enrole.log("script", "multiple matchs for eraliases=" + entryUid);
 var entryCn = subject.cn;
 if (typeof entryCn != "undefined") {
  Enrole.log("script", "checking cn=" + entryCn[0]);
  for (idx=0; idx<psResult.length; ++idx) {
   var cn1 = psResult[idx].getProperty("cn");
   if (cn1.length != 0 && cn1[0] == entryCn[0]) {
    /* we found a match for the cn */
    scriptResult = psResult[idx];
    break;
```

```
   }
  }
 }
 else {
  Enrole.log("script", "cn field not defined for eruid=" + entryUid);
 }
}
else {
 /* no person matched specified alias.
     See if there is a matching account uid in the company Active Directory */
 var acctSearch = new AccountSearch();
  /* Method acctSearch.searchByUidAndService(entryUid, masterServiceName) is used
       if the profile of the master service is same as the profile of the service
       for which the adoption policy is defined.
       If the profile of master service and the profile of the service for which the
       adoption policy is defined are different then the profile name of the master
       service is passed to the searchByUidAndService() method as follows–
       var asResult = acctSearch.searchByUidAndService(entryUid, masterServiceName,
       serviceProfileNameOfMasterService); */
   var asResult = acctSearch.searchByUidAndService(entryUid, masterServiceName);
   if (asResult != null && asResult.length == 1) {
  /* found a matching AD account -- use this accounts owner,
if it is not an orphan */
  var owner = asResult[0].getProperty("owner");
  if (owner.length == 1) {
   var owner_dn = owner[0];
   Enrole.log("script", "single match for service " + masterServiceName + " uid="
       + entryUid + ", returning person with dn=" + owner_dn);
   scriptResult = new Person(owner_dn);
  }
  else {
   Enrole.log("script", "service " + masterServiceName + " uid="
       + entryUid + " is an orphan");
  }
 }
 else {
  Enrole.log("script", "No match or more than one match for uid=" + entryUid
     + " on master service " + masterServiceName);
 }
}
return scriptResult;
/* end of script */
```

Example 3

The following example checks to see whether the name of a person, the gecos field in Linux, matches their full name in IBM Security Identity Manager, , and .

```
/*
 * OrphanAdoption JavaScript
 */

if (subject["gecos"] == null) {
    return null;
} else {
    var buf = "(|";

    for (i = 0; i < subject["gecos"].length; i++) {
        buf += "(cn=" + subject["gecos"][i] + ")";
    }

    buf += ")";

    var ps = new PersonSearch();
    /* Have to use sub-tree search type (2) */
    return ps.searchByFilter("Person", buf, 2);
}
```

Example 4

This example uses the new JavaScript API ExtendedPerson to adopt a "root" account as a "System" account and adopt other accounts as "Individual" accounts.

```
/*
 * OrphanAdoption JavaScript
 */

if ((subject[ "eruid"]==null)){
    return null;
} else if (subject["eruid"]!=null){
    var buff='(|';
    for (i=0;i<subject["eruid"].length;i++){
        buff+='(uid='+subject["eruid"][i]+')';
    }
    buff+=')';

    var ps = new PersonSearch();
    var searchResult = ps.searchByFilter("",buff, 2);
    if (searchResult!=null && searchResult.length==1) {
        var person = searchResult[0];

        // If it is a "root" account, adopt it as a "System" account;
        // otherwise, adopt it as an "Individual" account by default.
        if (subject.eruid[0] == "root") {
            return new ExtendedPerson(person, "System");
        } else {
            return person;
        }
    } else if (searchResult!=null && searchResult.length>1) {
        return searchResult;
    } else {
        return null;
    }
}
```

Changing an adoption policy

An administrator can change an adoption policy for specific services. For example, you might change an adoption policy to associate the policy with additional instances of a service type.

Before you begin

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

About this task

The effect of changes to an adoption policy can be seen when the next reconciliation is run. Changing an existing adoption policy does not affect existing accounts of the specific service or service type. Changes do not affect accounts that are already adopted. Only new and existing orphan accounts are adopted, based on the new policy.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Adoption Policies**.

   Note: To change a global adoption policy for a specific service type, you must navigate to **Configure System** > **Global Adoption policies**.

2. On the Work With Adoption Policies page, type information about the adoption policy or service in the **Search information** field. You can type an asterisk (*) as a wildcard.
3. Select a filter in the **Search by** field, and then click **Search**.
4. In the **Adoption Policies** table, locate and select the adoption policy that you want to change, and then click **Change**.
5. On the Manage Adoption Policies page, modify the information on the General, Service, and Rule pages.
6. Click **OK** to save the changes.
7. On the Success page, click **Close**.

Deleting an adoption policy

An administrator can delete an adoption policy for specific services.

Before you begin

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

About this task

Deleting an existing adoption policy does not affect existing accounts of the specific service or service type.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Adoption Policies**.
2. On the Work With Adoption Policies page, type information about the adoption policy or service in the **Search information** field. You can type an asterisk (*) as a wildcard.
3. Select a filter in the **Search by** field, and then click **Search**.
4. In the **Adoption Policies** table, locate and select an adoption policy that you want to delete, and then click **Delete**.
5. On the Confirmation page, review the adoption policy to delete, and then click **Delete**.
6. On the Success page, click **Close**.

Attribute matching

An adoption policy matches the attributes for an account on a managed resource to the attributes for an IBM Security Identity Manager user. If the match occurs, the account is assigned to the user so that the user owns the account. For example, the user can change the IBM Security Identity Manager account password. Otherwise, the account is identified as an orphan.

The default global adoption policy assigns an account to a user if the account user ID attribute matches the IBM Security Identity Manager user UID attribute.

Matching can use either single or multi-valued attributes. Matching occurs if the string value is identical to one of the following attributes:

- A single account attribute and a single user attribute
- Either a single attribute or any multi-valued attribute for either the account attribute or the user attribute

Account reconciliation and orphan accounts

Reconciliation uses an adoption policy to determine the owner of an account, or to identify the account as an orphan.

An adoption policy does not alter the ownership of accounts that are already owned within IBM Security Identity Manager.

Reconciliation uses either a global or a service-specific adoption policy. Reconciliation determines whether the user ID attribute for an account on a managed resource matches an alias attribute for a IBM Security Identity Manager user. If no match occurs, the account is identified as an orphan. Later, an administrator can manually assign orphan accounts to owners.

By default, during reconciliation, the global adoption policy is evaluated to determine the owner of an account by matching the account UID to the user UID.

Adoption policies can be defined at a global level, for a service type, or for a particular service instance. If more (or fewer) than one person is evaluated as the owner of the account, the account is orphaned.

Identity policies

An *identity policy* defines the characteristics of a user ID used when requesting a new account. An administrator defines the targets and the rule that is used to generate user IDs automatically for the services to which the rule is applied. The user ID can be based on attributes of the user for whom the account is being created.

An identity policy generates a default user ID used when requesting a new account. An administrator defines the rule to generate the user ID and specifies the service targets that apply.

Identity policies can be defined for the following targets:

All services
The same policy is used for all services.

Types of services
The policy is used for generating user IDs for services of the specified type.

Service instances
The policy is used for generating user IDs for the specified services.

Note: The default identity policy is used to generate the user ID when creating users, when the system is configured to provision Security Identity Manager accounts automatically to users.

A basic approach requires no scripting. You can define basic rules for an identity policy. Basic rules can specify which attributes to use, how many characters are used from each attribute, and what case to use when creating a user ID.

An advanced approach involves scripting, and you can use it to define more complex and customized rules. Security Identity Manager provides a default script you can modify. See the example section for an illustration of the advanced approach, which includes use of JavaScript.

To set a character limit, an identity policy rule defines the number of characters to use from a first and second attribute to form the user ID. Forming the user ID from the attributes has the following conditions:

- If the number of characters in the attribute is greater than the specified character limit, only the character limit is used.
- If the number of characters in the attribute is less than or equal to the specified character limit, the entire value of the attribute is used.
- If a second attribute is not specified, only the first attribute is used.
- If a duplicate user ID exists when Security Identity Manager creates a user ID, the process appends an integer to the new user ID to create a unique user ID.

An identity policy rule determines whether case modification occurs in forming a user ID. You can set the following conditions:

- Lowercase (default)
- Existing case
- Uppercase

If the identity policy generates a user ID with a null value, Security Identity Manager attempts to form a user ID. Security Identity Manager uses the first letter of the user's given name, concatenated with the value of the user's family name, retaining the existing case.

Name and **Business unit** are required fields when you are creating an identity policy. **Business unit** is populated with your organization name if you are authorized to create identity policies at the organization level. If you do not have that authority, the **Business unit** field is blank. You must search for a business unit where you have the authority to create an identity policy.

Identities

An *identity* is the subset of profile data that uniquely represents a person in one or more repositories, and includes additional information related to the person.

For example, an identity might be represented by a unique combination of the given, family, and full names of a person, and an employee number. The data might also contain additional information such as a telephone number, the office number, and an email address.

Identity policy script example (advanced approach)

Identity policies can be defined dynamically through the use of JavaScript (the advanced approach). Policies can also be defined with the basic method (which does not require any JavaScript). JavaScript can use all standard functions and programming constructs, including loops and conditional branches.

The values of personal attributes can be retrieved with the IBM Security Identity Manager specific JavaScript functions. The context of the script is a user (person) for whom the identity is being generated. A JavaScript object that represents the person within the IBM Security Identity Manager data model named subject represents this context.

The following example illustrates the advanced mode of creating user IDs with the uid attribute (or given name, if the uid attribute is empty) for an individual. The script also checks whether the user ID is already used. If the user ID is already in use, the script adds a number to the end of the user ID, making it unique.

```
function createIdentity() {
  var EXISTING_CASE = 0;
  var UPPER_CASE = 1;
  var LOWER_CASE = 2;
  var tf = false;
  var identity = "";
  var baseidentity = "";
  var counter = 0;
  var locale = subject.getProperty("erlocale");
  var fAttrKey = "uid";
  var sAttrKey = "";
  var idx1 = 0;
  var idx2 = 0;
  var fCase = 2;
  var sCase = 2;
  if ((locale != null) && (locale.length > 0)) {
    locale = locale[0];
  }
  if (locale == null || locale.length == 0)
    locale = "";
  var firstAttribute = "";
  var secondAttribute = "";
  if (((fAttrKey != null) && (fAttrKey.length > 0)) || ((sAttrkey != null)
  && (sAttrkey.length > 0))) {
    if ((fAttrKey != null) && (fAttrKey.length > 0)) {
      firstAttribute = subject.getProperty(fAttrKey);
      if (((firstAttribute != null) && (firstAttribute.length > 0)))
        firstAttribute = firstAttribute[0];
      if (firstAttribute == null || firstAttribute.length == 0)
        firstAttribute = "";
      else {
        firstAttribute = IdentityPolicy.resolveAttribute(fAttrKey,
        firstAttribute);
        if ((idx1 > firstAttribute.length) || (idx1 == 0))
          idx1 = firstAttribute.length;
        firstAttribute = firstAttribute.substring(0, idx1);
      }
      if (fCase == UPPER_CASE)
        firstAttribute = firstAttribute.toUpperCase(locale);
      else if (fCase == LOWER_CASE)
        firstAttribute = firstAttribute.toLowerCase(locale);
    }
    if ((sAttrKey != null) && (sAttrKey.length > 0)) {
      secondAttribute = subject.getProperty(sAttrKey);
      if (((secondAttribute != null) && (secondAttribute.length > 0)))
        secondAttribute = secondAttribute[0];
      if (secondAttribute == null || secondAttribute.length == 0)
        secondAttribute = "";
      else {
        secondAttribute = IdentityPolicy.resolveAttribute(sAttrKey,
   secondAttribute);
        if ((idx2 > secondAttribute.length) || (idx2 == 0))
          idx2 = secondAttribute.length;
        secondAttribute = secondAttribute.substring(0, idx2);
      }
      if (sCase == UPPER_CASE)
        secondAttribute = secondAttribute.toUpperCase(locale);
      else if (sCase == LOWER_CASE)
        secondAttribute = secondAttribute.toLowerCase(locale);
    }
    baseidentity = firstAttribute + secondAttribute;
  }
  if ((baseidentity == null) || (baseidentity.length == 0)) {
    var givenname = subject.getProperty("givenname");
    if (((givenname != null) && (givenname.length > 0)))
      givenname = givenname[0];
    if (givenname == null || givenname.length == 0)
```

```
      givenname = "";
    else
      givenname = givenname.substring(0, 1);
    baseidentity = givenname + subject.getProperty("sn")[0];
  }
  tf = IdentityPolicy.userIDExists(baseidentity, false, false);
  if (!tf) {
    return baseidentity;
  }
  while (tf) {
    counter+=1;
    identity = baseidentity + counter;
    tf = IdentityPolicy.userIDExists(identity, false, false);
  }
  return identity;
}
return createIdentity();
```

Creating an identity policy

An administrator can create an identity policy for use by all service types, specific service types, or specific service instances. For example, you can create an identity policy that specifies that a user ID is constructed from the family name of a user and a department number.

Before you begin

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

About this task

IBM Security Identity Manager offers two approaches, basic and advanced, for creating an identity policy. Decide which approach you want to use.

Note: If an identity policy is intended to specify a service instance as a target, that service instance must exist.

You can use the Manage Identity Policies notebook to create an identity policy. Identity policies do not change user IDs for accounts that exist. Rather, they are used when creating new accounts through Security Identity Manager.

Note: When you are defining a new identity policy, services that are already the target of an identity policy are listed. However, the services are not selectable from the services table on the Add Targets page. An error message is generated during the save operation if a target service type is already being used in another identity policy.

To create an identity policy, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Identity Policies**.
2. On the Work With Identity Policies page, in the **Identity Policies** table, click **Create**.
3. On the Manage Identity Policies page, on the General page, type a name and select a business unit for your identity policy.

Note: On the General Page, you can optionally specify a caption to provide additional information about the policy and a description of its purpose. You can specify keywords to reference the identity policy and a status. The status value is `enabled` to use the policy and make it active, or `disabled` to make the policy inactive. You can also specify a user type to which the identity policy applies. You can specify the extent to which the identity policy applies to a business unit or to a business unit and subunits.

4. Click the Targets page. Add one or more services or service types to which the identity policy applies, or specify that the policy applies to all service types:
   - To specify that the identity policy applies to all service types, select **All service types**.
   - To specify that the identity policy applies to specific service instances:
     a. Click **Add**.
     b. On the Add Targets page, specify your search criteria, and then click **Search**.
     c. In the **Services** table, select a service.

        Note: If you select the box at the top of the column, all services are targeted. To apply all service *types*, select **All Service Types**. If you select **All Service Types**, you cannot add specific service types or instances. If you want to apply the policy to selected service types or instances, ensure that **All Service Types** is not selected.
     d. Click **OK**.
   - To specify that the identity policy applies to a specific service type:
     a. Click **Add**.
     b. Select a Target type of Service type.
     c. Select the service type to which you would like the identity policy to apply.
     d. Click **OK**.

   The script field is populated with the default identity policy for the Person user type.
5. On the Manage Identity Policies page, click the Rule page to specify the schema attributes that the identity policy uses to create a user ID.
   - To use a basic input mode that applies a rule with schema attributes, select **Simple - define rule** and provide the following details:
     – A first attribute, its character limit, and its type of case (existing, upper, or lower)
     – (Optionally) a second attribute, its character limit, and its type of case (existing, upper, or lower)

     A blank value for character limit means no limit, and the entire attribute is used. If a duplicate user ID exists at the time an account is requested, an integer is appended to the user ID and incremented until a unique user ID is determined.
   - For the identity policy that uses JavaScript code, select **Advanced - define script**. The script field is populated with the default identity policy for the Person user type.
6. Click **OK** to save the changes.
7. On the Success page, click **Close**.

Changing an identity policy

An administrator can change an identity policy to meet your organizational requirements for user IDs. For example, you might change an identity policy to use the office number of a user when a new user ID is created.

Before you begin

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

About this task

Changes to the identity policy affect only new accounts; old accounts are not affected by these changes.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Identity Policies**.
2. On the Work with Identity Policies page, type information about the identity policy, service, or business unit in the **Search information** field, or use an empty value. Select a filter in the **Search by** field and click **Search**.
3. In the **Identity Policies** table, locate and select an identity policy, and click **Change**.
4. On the Manage Identity Policies page, modify the information on the General, Targets, and Rule pages. The business unit designation cannot be changed for an identity policy that is already created.
5. Click **OK** to save the changes.
6. On the Success page, click **Close**.

Deleting an identity policy

An administrator can delete an identity policy that is not needed to manage user IDs. Deleting an identity policy causes the services that are using the identity policy to use another identity policy. For example, the services use the default identity policy that applies to all services.

Before you begin

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

About this task

If an applicable identity policy is not defined and the identity policy of a service is deleted, the **user ID** field on the corresponding account form is blank.

To delete an identity policy, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Identity Policies**.
2. On the Work With Identity Policies page, type information about the identity policy, service, or business unit in the **Search information** field, or use an empty value. Select a filter in the **Search by** field, and click **Search**.

3. In the **Identity Policies** table, locate and select an identity policy, and then click **Delete**.
4. On the Confirm page, review the identity policy to delete, and then click **Delete**.
5. On the Success page, click **Close**.

Password policies

A *password policy* defines the password strength rules that are used to determine whether a new password is valid.

A *password strength rule* is a rule to which a password must conform. For example, password strength rules might specify that the minimum number of characters of a password must be 5. The rule might also specify that the maximum number of characters must be 10.

A password policy sets the rules that passwords for a service must meet, such as length and type of characters allowed and disallowed. Additionally, the password policy might specify that an entry is disallowed if the term is in a dictionary of unwanted terms. To select this choice in the user interface, you must first load a `dictionary.ldif` file into the IBM Security Identity Manager.

You can specify the following standards and other rules for passwords:

- Minimum and maximum length
- Character restrictions
- Frequency of password reuse
- Disallowed user names or user IDs
- Specify a minimum password age

Note:

- If password synchronization is enabled, the administrator must ensure that password policies do not have any conflicting password strength rules. When password synchronization is enabled, Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

  You might need to coordinate the password strength rules for the services. The first password strength rule might specify a minimum number of eight characters. Another password strength rule might specify a maximum number of *six* characters for a password. You must resolve such conflicts to enable a user to log on successfully.
- Some sites with a service such as AIX might require longer passwords for users who have root authority. You might set a value for the minimum length of a password that is shorter than the default password on the AIX server. The shorter value might cause some users with root authority to enter a password that is shorter than required, causing authentication failure.

Creating a password policy

An administrator can create a password policy for use with one or more services. For example, you might create a password policy that specifies a rule that a character can be repeated no more than three times in a password.

Before you begin

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

Before you create a password policy, create one or more service instances to associate with the password policy. If your policy uses a dictionary of unwanted terms, create and import the dictionary file also.

About this task

If a password policy exists for all services, other policies can still be added. However, only a single password policy can be specified for each service type or each instance of a service type. A password policy might exist for a service type. Additionally, password policies might exist for different instances of that service type. The more specific password policy overrides all others (for example, a password policy for a Windows service instance overrides a password policy for the Windows service).

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.
2. On the Select Password Policies page, in the **Password Policies** table, click **Create**.
3. On the Manage Password Policies page, on the General page, type a name and select a business unit for your password policy. Optionally, you can add information about the scope of the policy, its status, keywords, a caption, and a description for the password policy.
4. Click the Targets page, and then choose to add all service types or choose one or more specific services to associate with the policy. To add one or more services, complete these steps:
   a. Click **Add**.
   b. On the Add Targets page, type your search criteria, and then click **Search**.
   c. In the **Services** table, select one or more services.
   d. Click **OK**.

   Note: Service type can also be selected as target for password policy by selecting the target type as Service Type.
5. On the Manage Password Policies page, click the Rules page. Specify the settings for the password rules that you want to use to determine whether a password entry is valid.

   Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.
6. Click **OK** to save the changes.
7. On the Success page, click **Close**.

Adding targets to a password policy

An administrator can add targets to an existing password policy.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.
2. On the Select Password Policies page, type information about the password policy, service, or business unit in the **Search information** field. You can also use an asterisk (*) as a wildcard.
3. Select a filter in the **Search by** field, and click **Search**.
4. In the Password Policies table, locate and select a policy, and then click **Change**.
5. Click the Targets page, and either add all service types or select one or more specific services to associate with the policy.

   To add one or more specific services:

   a. Click **Add**.
   b. On the Add Targets page, type your search criteria, and then click **Search**.
   c. In the **Services** table, select one or more services.
   d. Click **OK**.

   Note: A specific Service type can also be selected as a target for password policy by selecting the target type as Service Type.
6. Click **OK** to save the changes.
7. On the Success page, click **Close**.

Creating a password policy rule

As an administrator, you can create a rule for an existing password policy. For example, you might create a rule that specifies the minimum number of numeric characters for a password.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.
2. On the Select Password Policies page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. On the Manage Password Policies page, click the Rules page. Specify the settings for the password rules that you want to use to determine whether a password entry is valid.

   Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM

Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

5. Click **OK** to save the changes.
6. On the Success page, click **Close**.

Changing a password policy

An administrator can change a password policy to meet the requirements of your organization for passwords. For example, you might change a password policy to set the minimum and maximum characters that are required for the password.

Before you begin

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

About this task

Changes to the password policy affect only new accounts. Old accounts are not affected by these changes.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.
2. On the Select Password Policies page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (`*`). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. On the Manage Password Policies page, modify the information on the General, Targets, and Rules pages.

   Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.
5. Click **OK** to save the changes.
6. On the Success page, click **Close**.

Changing targets for a password policy

An administrator can change targets for an existing password policy.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.

2. On the Select Password Policies page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. Click the Targets page. Add or remove all service types or choose to change one or more specific services that are associated with the policy. To change one or more specific services:
   a. Click **Add**.
   b. On the Add Targets page, type your search criteria, and then click **Search**.
   c. In the **Services** table, select or clear one or more services.
   d. Click **OK**.
5. Click **OK** to save the changes.
6. On the Success page, click **Close**.

Changing a password policy rule

An administrator can change a password policy rule. For example, you might change or remove the settings for an existing rule.

Before you begin

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

About this task

To change a password policy rule, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.
2. On the Select Password Policies page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.

   Note: If the search for password policies is done by Service, the default Service Owner ACIs limit the search to the password policies in Services that belong to the Service Owner. However, these default ACIs do not limit the search by password policy name. The default ACIs can be modified, or new ACIs can be created to change the search scope for the Service Owner.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. On the Manage Password Policies page, click the Rules page. Change or remove the settings for the password rules that you want to use to determine whether a password entry is valid.

   Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM Security Identity Manager combines policies for all accounts owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.
5. Click **OK** to save the changes.

6. On the Success page, click **Close**.

Deleting a password policy

An administrator can delete a password policy that is no longer needed to control password entries.

Before you begin

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

About this task

Deleting a password policy causes the services that are using the password policy to use another password policy, such as the default password policy.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Password Policies**.
2. On the Select Password Policies page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (`*`). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Delete**.
4. Click **OK** to save the changes.
5. In the Success page, click **Close**.

Customized password rules

You can use IBM Security Identity Manager server to add customized logic for generating passwords. To add the logic you can use a customized rule, a customized generator, or a combination of both.

Adding customized logic for password rules with a customized rule

A customized password rule is used for validating both new passwords that are generated by IBM Security Identity Manager Server and existing passwords.

Before you begin

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

Procedure

1. Create a class by implementing *com.ibm.passwordrules.Rule interface*.
2. Register the class in `passwordrules.properties` by entering a line like the following one:

   ```
   password.rule.com.ibm.tivoli.itim.CustomPasswordRule1=true
   ```

   The value of this expression determines the type of interface widget that is used to create a customized rule when you define a password policy. The following values are valid:

   - A value of `true` means that the instantiated rule object requires a parameter. The widget is a text box. If any value is entered, a customized rule is used. If the value is optional, typing in any printing character marks the rule for use.

- A value of `false` means that the rule does not require parameters. If the box is selected, a customized rule is used.

If more than one parameter value is required, a user-defined delimiter might separate individual values. Alternatively, the value might contain a structure that is represented by a user-defined XML document.

3. Optional: Add a label for the customized rule name. The key for the value is the fully qualified name of the customized class. The specified value is displayed on all screens that show the password rules `password.rule.com.ibm.tivoli.itim.CustomPasswordRule1=Use Complexity Level 1`. In this example, the required prefix is followed by the fully qualified name of the customized rule class. Both parts constitute the entire property key for any customized rule.

   Note: If the customized label is not defined in `CustomLabels.properties`, the fully qualified name of the customized Java class is displayed on the interface forms.

Adding a customized password generator

You can add a customized password generator for creating passwords with the IBM Security Identity Manager Server.

Before you begin

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

Procedure

1. Create a customized password generator class that implements the *com.ibm.passwordrules.PasswordGenerator* interface.
2. Register the customized password generator class. The customized password generator might be used by adding a line to the `passwordrules.properties` file. For example:

   ```
   generator.ibm.tivoli.itim.CustomGenerator
   ```

   In this example, `generator` is the required prefix followed by the fully qualified name of the password generator class. Both parts constitute the entire property key of a customized generator. Initialization parameters can be passed to the customized generator by specifying a value for the property, as in the following example:

   ```
   generator.ibm.tivoli.itim.CustomGenerator=value1?value2
   ```

   This value must be defined in a format that is expected by the *initialize()* method of the generator. If the author of a customized generator class chooses not to do any initialization, the property value is ignored by the initialize method of the generator class.

   Note: Any password generator, including the built-in one, has a global scope, and is the only one that generates passwords for accounts of all service types.

Customized logic using customized rules and a customized generator

You can use a combination of a customized rule and a customized generator to add customized logic for generating passwords.

Using standard password rules might not always be helpful or even wanted at all. You might prefer a single customized password rule to generate compliant passwords. You might use a standard set of password rules to define password policies. When you want to avoid standard rules, that preference must be known to the IBM Security Identity Manager administrator.

Mixing customized rules with a customized generator might have unforeseen implications. For example, a customized password generator implementation might be sufficient to generate valid passwords, and thus a password policy might not be required at all.

Using a customized rule might preclude the authors of password policies from using some or even all standard password rules that might be incompatible with the customized rule. However, to achieve the wanted effect, authors of customized rules or generators might decide to use a combination of both. Such an approach might be more flexible, because different parameters can be passed to individual rule definitions in password policies for different service types.

Joining rules

Any class that implements a Rule interface is expected to provide logic in its join() method. This logic joins parameters of two rules of the same type defined for two or more accounts of different service types. If such joins are difficult or even impossible to do, parameters of one of the two similar rules can be chosen by code. The Framework does not provide any mechanism for resolving join conflicts. The author of customized rule classes resolves such conflicts by imposing a preferred mechanism in the join() method itself.

Constraining the password generator

For customized password generators, which are based on an iterative algorithm, limiting the possible number of attempts during which the password might be generated is a way of ensuring that the maximum limit of iterations is not exceeded before a valid password is produced. A *valid password* is one that complies with all the rules defined for it in a password policy. Each rule class implements the constrain() method that tells the generator how to generate the password.

Authors of customized rule classes might choose not to implement the constrain() method. These authors must test the process of generating the expected password. They must test with a combination of rules, including the customized rules, which are expected to be used in production environment. The test must produce an acceptable, large number of consecutive passwords are generated without triggering the IterationsExceededException. If the test is successful, the mechanism is acceptable, and can be used in the production environment. Some customized password generators (for example, those generators based on a dictionary) might not require constrains at all. In such cases, constraint() methods although always called, do not affect the way passwords are generated.

Note: The maximum limit of iterations is hardcoded 20,000.

Internationalization

Parameter values passed to the customized generator might include Unicode characters. If the `passwordrules.properties` file contains any Unicode characters, save it in Unicode format. IBM Security Identity Manager automatically detects the

format when the file is read. A file that contains Unicode characters must be viewed and edited with a text editor that can display these characters.

Alternatively, use the hex-encoded format to insert the Unicode characters into the file: `\uXXXX` or `0xXXXX`. This method makes it possible to view and edit the file in text format, but the generator class must interpret these character encodings. The StandardGenerator class in the password rules framework can generate passwords using Unicode characters to the extent supported by the Java virtual machine used with the IBM Security Identity Manager server.

The default character set used by the StandardGenerator class is uppercase and lowercase letters from the Latin alphabet. They correspond to Unicode ranges 0x0041-0x005a and 0x0061-0x007a, and most special characters such as #, $, and % that are in the ASCII set. You can extend or replace this character set by defining a parameter value for the standard generator class in the `passwordrules.properties` file. For example:

```
generator.com.access360.passwordrules.standard.StandardGenerator=
\0x0041,0x005a \0x0061,0x007a  \0x0104,0x0107  \0x0118,0x0119  \0x00d3
\0x00f3  \0x0141,0x0144  \0x015a,0x015b  \0x0179,0x017c
```

The first two ranges are the standard Latin letters. The others are from Extended Latin I and II Unicode sets. Customized rule parameter values added to password policy definitions might also be required to accept Unicode characters. Again, the two ways of specifying the Unicode values and ranges of values apply here as well. XML is used to save all rules within a password policy to the LDAP directory. The interface always displays the customized rule parameters exactly as they were entered.

Configuration of minimum password age rule

An administrator can configure a minimum password age rule to limit how frequently users can change the password on their account. This rule is provided in the password policy. By default, the rule is disabled.

The following points describe the limitations, scenarios, and configuration information about the minimum password age rule.

- The rule accepts only integer values. A user with permissions to define or edit a password policy can specify the minimum period, in hours, for a password change. A user cannot change the password on that account again within the specified period.
- IBM Security Identity Manager interprets the specified integer value for the rule in hours. Security Identity Manager does not evaluate the rule when a user specifies a negative value, `0`, or no value. In other words, users can change the password on their accounts immediately.
- Security Identity Manager can evaluate the rule only in these conditions:
  - When users try to change the password on any of the accounts owned by them.
  - When the previous password change on those accounts was successfully run by the same users (owners of the accounts).

  In other words, Security Identity Manager does not evaluate the rule if users other than owners of the accounts made the previous account password change. For example, help desk or system administrators.
- Security Identity Manager does not evaluate the rule when users change the password on accounts that are not owned by them. For example, Security

Identity Manager does not evaluate the rule when help desk or system administrators change the password on some other user accounts. Security Identity Manager does not evaluate the rule if the password change is initiated by the system. For example, a password change initiated by the lifecycle rule or an automatic provisioning request workflow.

- Security Identity Manager maintains this information in IBM Security Directory Server:
  - Users who ran the last password change on each account object.
  - Time when the password change was run on each account object.

  For some reasons, if this information is corrupted or these attributes are wiped off from the account object, then Security Identity Manager does not evaluate the rule correctly.
- Security Identity Manager stores the password change information only when the password change is initiated by using one of these resources:
  - IBM Security Identity Manager console
  - IBM Security Identity Manager Self Service or the Identity Service Center user interface
  - IBM Security Identity Manager APIs

  Therefore, any information about password changes done directly on the resource or by using some other tool is not used to evaluate the rule.

Adding a customized minimum password age rule:

An administrator can add a customized minimum password age rule to limit users from changing the password on their account. For example, you might want to specify the minimum time, in hours, for a password change on your account before you can change it again.

Before you begin

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

Ensure that IBM Security Identity Manager is installed.

About this task

Run the following procedure to configure and enable this rule in your environment.

If you are on a clustered environment, then repeat the following procedure on each node of the cluster. The procedure configures and enables this rule in your environment.

Note: By default, this rule is disabled.

Procedure

1. Stop WebSphere Application Server.
2. Change to the directory where the `passwordrules.properties` file is located. For example: `$ISIM_HOME/data`.
3. Uncomment the following property in `passwordrules.properties` files to enable the new rule:

```
password.rule.com.ibm.passwordrules.standard.MinAgeConstraint=true
```

The "Minimum Password Age" label is added in the $*ISIM_HOME*/data/CustomLabels.properties file.

Note: *ISIM_HOME* is the directory where Security Identity Manager is installed.

4. Optional: Complete these steps if a language pack is installed, or if the com.ibm.passwordrules.standard.MinAgeConstraint key is not assigned a label in the CustomLabels_nn.properties file:
   a. Edit the appropriate $*ISIM_HOME*/data/CustomLabels_*nn*.properties file if a language pack is installed. *nn* is a two letter language code. For example, en for English.
   b. Add the following line at the end of the file with appropriate messages for that language. Add the line after you replace the text on the right of the equals "=" sign. For example:

      ```
      com.ibm.passwordrules.standard.MinAgeConstraint
      =Minimum Password Age
      ```

      Do not change the English text on the left of the equals "=" sign.
5. Change to the directory where the tmsMessages.properties file is located. For example: $*ISIM_HOME*/data.
6. Back up the tmsMessages.properties file.
7. Using any text editor, open the tmsMessages.properties file.
8. Add the following message at the end of the tmsMessages.properties file. For example:

   ```
   com.ibm.passwordrules.MinAgeConstraint.MIN_AGE_VIOLATED
   =Attempting to set the password within minimum age of password.
   ```

   If you violate the rule, this message displays on the IBM Security Identity Manager Console.
9. Save the tmsMessages.properties file and close the editor.

   Note: Repeat Steps 5, 6, 7, 8, and 9 to edit the tmsMessages_nn.properties file for the language packs that you installed.
10. Start WebSphere Application Server.

Results

The **Rule** tab on the Manage Password Policies page displays the **Minimum Password Age** rule.

What to do next

Specify appropriate values for the minimum password age.

Provisioning policies

A *provisioning policy* grants access to many types of managed resources, such as IBM Security Identity Manager Server, Windows NT servers, and Solaris servers.

Each provisioning policy consists of the following components:

- General Information

- Membership
- Entitlements

A provisioning policy must target one or more service instances, service types, or a service selection policy. System administrators can use provisioning policy parameters to define attribute values that are required and values that are optional.

A provisioning policy defines the accounts and access that are authorized to users or automatically provisioned for users by the user's role. When account and access are authorized to a user by a provisioning policy, they can be requested by the user. A provisioning policy can be used to support role-based provisioning, in which accounts and access are automatically provisioned to a user, based on the user's roles.

Provisioning policies are important to support security compliance. Security Identity Manager evaluates all account and access requests based on the provisioning policy to identify accounts and access that are not authorized and take appropriate actions to handle noncompliant account and access. Based on the enforcement configuration on the service, Security Identity Manager can either mark the account or access as noncompliant. Security Identity Manager can also suspend the account, alert the administrator to revoke disallowed privilege, or automatically correct the account or access and make it compliant. A provisioning policy provides a key part of the framework for the automation of identity lifecycle management.

Security Identity Manager provides APIs that interface to information about provisioning policies defined in Security Identity Manager, and interface to the access granted to an individual task. These APIs can be used effectively to generate audit data.

When two or more provisioning policies are applied to the same user, a *join directive* defines how to handle attribute values from different policies. To work with policy joins or customize them, go to the navigation tree and select **Configure System > Configure Policy Join Behaviors**.

Provisioning policies can be mapped to services of a distinct portion or level of the organizational hierarchy. The business unit to which the provisioning policy belongs determines the services the policy governs. The scope of the provisioning policy indicates whether to cover services in the same level of the business unit or the subtree of the business unit. An entitlement in the provisioning policy support different types of service targets. Target types include all services, services of same type, services defined by service selection policy, or a specific service instance. In all cases, the services must be within the specified scope of the business unit where the policy is defined. A service selection policy enables service selection base on person attributes.

Policy enforcement

Policy enforcement is the manner in which IBM Security Identity Manager allows or disallows accounts that violate provisioning policies.

When a provisioning policy, person, account data, or dynamic role is changed, an account that was originally compliant with a provisioning policy can become noncompliant.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

When a policy enforcement action is set to `Global`, the policy enforcement for any service is defined by the global or default configuration setting.

You can set the policy enforcement action as **Mark**, **Suspend**, **Correct**, **Alert**, or **Use Global Enforcement Action: Mark**. For more information, see *Policy enforcement actions* in "Policy enforcement" on page 159.

Provisioning policy parameter enforcement rules

The parameter enforcement types specify the rule for the system to evaluate the validity of an account attribute value.

An account that contains an invalid value is considered a noncompliant account. The role of the policy enforcement settings (`Mark`, `Suspend`, `Correct`, and `Alert`) is to specify the action the system does when the account becomes noncompliant. A `Correct` policy enforcement setting causes the system to take corrective action for the noncompliant account. Actions, include adding mandatory values to the account and removing invalid values from the account.

Use the following key to determine the enforcement type:

M Mandatory

A Allowed

D Default

E Excluded

A mandatory value is added if it is missing from an account. Default attributes are used only during account creation. Afterward, they can be used. Excluded attribute values are removed only if they are not granted in another policy.

The following table lists the set of valid and mandatory parameter values.

Table 83. System attribute enforcement rules

ALLOWED				ACTIONS	
M	**A**	**D**	**E**	**Account creation**	**Account validation (reconciliation)**
				No action.	All valid values.
X				Mandatory attributes are set.	Mandatory attributes are set to the defined value, and all other values are not valid.
	X			No action.	All defined attributes are valid, and all others are not valid.
		X		Default attributes are set.	Default attributes defined are defaulted on account creation, and all other values are also valid.
			X	No action.	Excluded attribute values are removed (all other values can be present or set on the attribute). The valid values are equal to {M + A + D + not(E)}. If a value is not contained in the set of valid values, it is removed. **Note:** Excluded adds values by negation to the allowed set. It does not remove values from the allowed set.
X	X			Mandatory attributes are set.	Mandatory attributes are set to the defined value. Valid values can be present or set on the attribute.

Table 83. System attribute enforcement rules (continued)

ALLOWED				ACTIONS	
M	**A**	**D**	**E**	**Account creation**	**Account validation (reconciliation)**
X	X	X		Mandatory and default attributes are set.	Mandatory attributes are set to the defined value. Optional and default values can be present or set on the attribute.
X	X	X	X	Mandatory and default attributes are set.	Mandatory attributes are set to the defined value. Excluded attribute values are removed. Optional and default values can be present or set on the attribute.
X		X		Mandatory and default attributes are set.	Mandatory attributes are set to a defined value. Default values can be present or set on the attribute.
X		X	X	Mandatory and default attributes are set.	Mandatory attributes are set to a defined value. Default values can be present or set on the attribute. Excluded attribute values are removed.
X			X	Mandatory attributes are set.	Mandatory attributes are set to defined values. Excluded attribute values are removed (all other values can be present or set on the attribute).
X	X		X	Mandatory attributes are set.	Mandatory attributes are set to defined values. Optional attributes are valid, and must be one of the defined values if a value is set. Excluded attribute values are removed (all other values can be present or set on the attribute).
	X	X		Default attributes are set.	Optional attributes are valid and must be one of the defined values if a value is set. Default attributes are valid.
	X	X	X	Default attributes are set.	Optional attributes are valid, and must be one of the defined values if a value is set. Default attributes are valid. Excluded attribute values are removed (all other values can be present or set on the attribute).
	X		X	No action.	Optional attributes are valid, and must be one of the defined values if a value is set. Excluded attribute values are removed (all other values can be present or set on the attribute).
		X	X	Default attributes are set.	Default attributes are valid. Excluded attribute values are removed (all other values can be present or set on the attribute).

Creating a provisioning policy

An administrator can create a provisioning policy.

Before you begin

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

Organizational roles and services that the provisioning policy uses must be in place before you add the provisioning policy.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Provisioning Policies**.

2. On the Manage Provisioning Policies page, in the **Provisioning Policies** table, click **Create**.
3. On the Manage Provisioning Policies page, on the General page, type a name and a priority number, and select a business unit for your provisioning policy. Optionally, you can also specify the scope, a caption, a description, keywords, and the policy status.
4. Click the Members page, and select the member type that you want to associate with the provisioning policy. If you select **Roles specified below**, complete these steps to add one or more roles to the **Roles** table:
   a. Click **Add**.
   b. On the Organizational Role page, specify your search criteria, and then click **Search**.
   c. In the **Roles** table, select one or more roles.
   d. Click **OK**.
5. On the Manage Provisioning Policies page, click the Entitlements page, and add one or more entitlements to the provisioning policy:
   a. Click **Create**.
   b. On the Account Entitlement page, select the provisioning option, ownership type, target type, and a workflow. Select the service type and service, if applicable.
   c. Click **OK**.
6. Click **Submit** to save the policy.
7. On the Schedule page, choose to create the provisioning policy immediately or select a specific date and time. Then, click **Submit**.
8. On the Success page, click **Close**.

Changing a provisioning policy

As an administrator, you can modify a provisioning policy.

Before you begin

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

About this task

System administrators can modify provisioning policies by changing the policy definition, membership, or entitlement.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Provisioning Policies**.
2. On the Manage Provisioning Policies page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Change**.

4. On the Manage Provisioning Policies page, modify the information on the General, Members, and Entitlements pages.
5. Click **Submit** to save the changes.
6. On the Schedule page, indicate whether to change the provisioning policy immediately or select a specific date and time. Then, click **Submit**. You can indicate to submit changes only, or to submit the entire policy.
7. On the Success page, click **Close**.

Previewing a modified provisioning policy

An administrator can preview the effect of a provisioning policy on users before adding, modifying, or deleting the policy.

Before you begin

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

About this task

Previewing a provisioning policy provides you with a summary of the number of accounts that are affected and specific details for each account that the policy impacts. The provisioning policy preview provides details about the accounts that are:

- Provisioned
- Suspended
- Deleted
- Modified
- Marked as noncompliant
- Get a changed status from noncompliant to compliant

If the results of the preview are what you expected, you can continue submitting and activating the policy. If the results of the preview are not what you expected, you can revise the policy.

When you preview a modified policy, you can choose to have IBM Security Identity Manager compute the impact of the entire policy on all users that belong to policy memberships. Alternatively, you can choose to compute only the impact of the changes you made to the policy. For example, you modified an existing provisioning policy to include a newly defined role. You might want to preview the results of the modified policy selectively as they apply to users who were assigned to that role.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

If you change the ownership type of a service policy entitlement, accounts are evaluated based on that ownership type. Accounts with a different ownership type than the one specified in the changed entitlement are disallowed on that service. The exceptions are if you change the ownership type to All or the ownership type is covered by another entitlement on the same policy. In those cases, the accounts are not disallowed.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Provisioning Policies**.
2. On the Manage Provisioning Policies page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Change**.
4. On the Manage Provisioning Policies page, modify the information about the General, Members, and Entitlements pages, and click **Preview**.
5. On the Preview Policy Enforcement page, select **Enforce changes only** or **Enforce entire policy**.
6. Click **Continue**.

   The preview is generated and displayed on the Preview Policy Summary page, which is categorized by the following states:

   - Disallowed accounts
   - Noncompliant accounts
   - Compliant accounts

   Click a category of account changes to view the individual accounts that the policy changes affect.
7. On the Preview Policy Summary page, click **Close**.

What to do next

After you determine that the effects of the policy changes are acceptable, the changes can be submitted to the system.

Creating a draft of an existing provisioning policy

As an administrator, you can modify an existing provisioning policy and save the modified policy as a draft, without committing the changes to the system.

Before you begin

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

You might save an existing provisioning policy as a draft. Both the original and the draft versions are listed on the Manage Provisioning Policies page in the **Provisioning Policies** table. When you commit the draft version to the system, it replaces the original, which is removed from the system, along with the draft version.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Provisioning Policies**.
2. On the Manage Provisioning Policies page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and then click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Change**.

4. On the Manage Provisioning Policies page, modify the information on the General, Members, and Entitlements pages.
5. Click **Save as Draft**.
6. On the Success page, click **Close**.

Committing a draft provisioning policy

As an administrator, you can commit a provisioning policy draft.

Before you begin

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

When you commit a draft version to the system, it replaces the original provisioning policy, which is removed from the system, along with the draft version.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Provisioning Policies**.
2. On the Manage Provisioning Policies page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy draft, and click **Change**.
4. On the Manage Provisioning Policies page, click **Submit** to commit the draft.
5. On the Schedule page, indicate whether to change the provisioning policy immediately or select a specific date and time. Then, click **Submit**.
6. On the Success page, click **Close**.

Deleting a provisioning policy

An administrator can delete a provisioning policy. Deleting a provisioning policy removes all accounts that this policy created.

Before you begin

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

Before you delete a provisioning policy, confirm that you want to delete all the memberships and entitlements that are contained in that policy. If a role is a child role of another organizational role in a provisioning policy, then that child role also inherits the permissions of provisioning policy. Therefore, when you delete a provisioning policy, the permissions of the child roles might be deleted or suspended.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Provisioning Policies**.

2. On the Manage Provisioning Policies page, type information about the provisioning in the **Search information** field, or type an asterisk (*) and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Delete**.
4. On the Confirm page, review the provisioning policy to be deleted, choose a date and time for the deletion to occur, and click **Delete**.
5. On the Success page, click **Close**.

Managing provisioning policies by role

As an administrator, you can manage provisioning policies that are associated with roles.

Before you begin

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

About this task

System administrators can manage provisioning policies that are associated with roles.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

Procedure

1. From the navigation tree, select **Manage Roles**. The Manage Roles page is displayed.
2. On the Manage Roles page, complete these steps:
   a. Type information about the role in the **Search information** field.
   b. In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**. A list of roles that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
3. In the **Roles** table, click the icon (▸) next to the role, and then click **Manage Provisioning Policies**. The Work With Provisioning Policies page is displayed.
4. On the Work With Provisioning Policies page, you can create, change, or delete provisioning policies.
5. When you are finished managing the provisioning policies, click **Close** to close the page.

Recertification policies

Recertification simplifies and automates the process of periodically revalidating a target type (account or access) or a membership (role or resource group). The recertification process validates whether the target type or membership is still required for a valid business purpose. The process sends recertification notification and approval events to the participants that you specify. A *recertification policy*

includes activities to ensure that users provide confirmation that they have a valid, ongoing need for a specified resource or membership.

A recertification policy defines how frequently users must certify their need for a resource or membership. The policy also defines the operation that occurs if the recipient declines or does not respond to the recertification request. Recertification policies use a set of notifications to initiate workflow activities that are involved in the recertification process.

There are three recertification target types:

- User
- Account
- Access

A user recertification, unlike an account or access recertification, allows you to certify roles, accounts, and groups (which include accesses) for the specified user within a single activity.

A recertification policy is implemented as a workflow. A default workflow is automatically built for simple policies. A recertification policy can prompt a recipient, such as a manager or system administrator to certify periodically that users still need to use accounts. The workflow generates an e-mail notification of the work item to be completed for recertification and generates To Do activities to request that the participant accept or reject the recertification.

A service owner can create a recertification policy for services and accesses that are administered by the user. A system administrator can create a recertification policy for all users, services, and accesses. For example, as an administrator, you can define a recertification policy that sets a 90-day interval for account recertification. If the recipient of the recertification request declines recertification, the account is suspended. The owner of the account that was rejected during recertification is notified by email based on the message template configured in the policy.

The recertification policy access control item (ACI) controls what a user can view or do with recertification policies. IBM Security Identity Manager provides default access control items that target recertification policies. The following table shows how changes to the default ACIs affect what you can see or do with the policies.

Table 84. Recertification policies and access control items

Who is permitted	Target object and access control item	Effect
Service owner group	Recertification policy - add, modify, remove, or search	Allows service owners to manage recertification policies.
Auditor or manager group	Recertification policy - search	Allows members of the auditor group or manager group to search or view recertification policies.
Auditor, manager, or service owner groups	Reports (recertification pending, history, and policies) run operation	Allows members of these groups to view these reports.

Audits that are specific to recertification are created for use by several reports that are related to recertification:

Accounts or access pending recertification
Provides a list of recertifications that are not completed.

Recertification change history (for accounts and accesses)
Provides a historical list of recertifications.

Recertification policies (for accounts and accesses)
Provides a list of all account and access recertification policies.

User recertification history report
Provides a historical list of user recertifications.

User recertification policy definition report
Provides a list of user recertification policies.

Resource selection for recertification

Security Identity Manager does not select accounts for recertification in the following circumstances:

- The ITIM Service account of the ITIM administrator (the actual name of the account and service inside Security Identity Manager) is not selected for recertification so that it is not deleted or suspended inadvertently. Any other ITIM account can be selected.
- Orphan accounts, which are accounts with no owners, are not selected for recertification.
- Account and access recertification policies do not select resources if the rejection of the resource results in the same operation. For example, if the rejection action is to suspend the accounts, the recertification policy does not select accounts that are already suspended because the rejection of the recertification would suspend the accounts, which has already occurred. If the rejection action is to delete the accounts after the accounts are suspended, the accounts are selected for recertification because a different action, such as deleting the suspended accounts, had not already occurred.

Recertification policy targets

Recertification policies can target various resources and memberships. Account recertification policies target accounts on specific services. Access recertification policies target specific accesses. User recertification policies can target a combination of role memberships, accounts on services, and groups on services (including groups defined as access).

There is a restriction with account and access policies:

- A service can be a member of only one account recertification policy
- An access can be a member of only one access recertification policy

These restrictions do not apply to user recertification policies. A user recertification policy might include services or accesses that are already part of another policy.

Recertification policy configuration modes

The configuration mode determines how you build the policy. The following modes are available:

Simple
If you use the simple mode, a workflow is automatically built, using the options that are selected on the Policy page.

Advanced

If you use the advanced mode, the workflow designer is launched with a simple workflow defined as the base configuration, using the options selected on the Policy page. The workflow can be further customized for business needs.

Note: If a policy is changed from simple to advanced mode, the policy cannot revert to a simple state without losing changes. The policy reverts to the default simple recertification workflow.

Viewing recertification status

Recertification requests can be viewed in **View Requests**. To find recertification requests, select the **View All Requests By Service** view or **View All Requests** view.

For services, see the option in the task list by service to view Account Recertification Status, and navigate to **Manage Services > Select a Service**. Click the icon adjacent to a service name and select **Account Recertification Status** to get to the status page.

For group access entitlements, to view Access Recertification Status, navigate to **Manage Groups > Select a Service**. Select the service and click **OK**. Then, click the icon adjacent to the group for the accesses and select **Access Recertification Status**.

Note: On the service protection category for ACIs is a new operation called Recertification Override that specifies which users can view and override the recertification status of an account. A similar ACI exists on the group protection category to specify which users can view and override the recertification status of an access.

Recertification policies and reports

Recertification reports can be requested by system administrators, service owners, managers, and auditors, based on ACIs. Included are reports of the following types:

- Accounts/Access Pending Recertification Report
- Recertification Change History Report
- Recertification Policies Report
- User Recertification History Report
- User Recertification Policy Definition Report

The actions taken during an account or access recertification policy run are stored in a database table RECERTIFICATIONLOG that is referenced by the recertification history report.

The actions taken during a user recertification policy run are stored in database tables named USERRECERT_HISTORY, USERRECERT_ROLE, USERRECERT_ACCOUNT, and USERRECERT_GROUP, which are referenced by the user recertification history report.

Note: Recertification audit events are generated from recertification policy workflows only, rather than from operational workflows.

Recertification activities

A *recertification activity* is displayed in the to-do list, and you can use it to approve or reject a user's need for a membership or access to a resource.

While recertification is underway, the user can continue to use the target type in question. If recertification is rejected, the account, access, group membership, or role membership might be marked, suspended, or deleted based on the configuration of the policy. The recertification approval activity does not necessarily go to the account owner. The participant can be specified using the **Who approves recertification** field in the **Policy** tab. Approvers can be the account owner, administrator, service owner, manager, user, organizational role, group, or access owner, depending on the specific type of recertification policy.

Depending on the policy configuration, the to-do task does not necessarily require completion. For example, the policy can be configured to take the positive path for approving recertification, so that if no action is taken on the to-do task, continued use is approved.

Note: You can set the **Timeout** action on the **Policy** tab to dictate the behavior.

Based on provisioning policy configuration, certain accounts and groups might be omitted from a user recertification activity even when the accounts and groups are within the scope of the user recertification policy. For example, groups that are mandatory on an account are always omitted from the activity. Accounts that are automatically provisioned for the user are also omitted from the activity as long as the user does not have additional accounts on the same service. If the user has multiple accounts on an automatically provisioned service, all the accounts are displayed in the user recertification activity. The recertifier must recertify at least one of the accounts on the service to submit the activity. Some accounts might be displayed in the activity for display purposes only if the accounts themselves do not require recertification, but have groups that require recertification.

Run option

You can click **Run** on the recertification policy management interface to cause the recertification policy to be evaluated on demand.

Note: Any schedule that is defined inside the policy remains intact if you click **Run**. The scheduled evaluation occurs regardless of whether **Run** was recently performed on demand. If you want to run the policy on demand only, disable the policy so that the scheduled evaluation does not occur.

Recertification message templates and schedule

A recertification policy defines the content of an email notification to participants and the interval that triggers a request for recertification.

The email notification alerts you to recertify a need for a specified membership or access to a resource. The action to be taken when the user does not complete the request by the due date is specified using the **Timeout Action** setting, which is set to `Approve` by default.

Note: If the recertification is approved or rejected, you can provide optional text for justifying the rejection. The text that is entered in the to-do list is audited, and can be seen in the Recertification Change History report or the User Recertification History report, depending on the type of policy.

You can create customized message templates for the recertification email and the rejection email.

The recertification email goes to the person who is responsible for recertification and approves recertification. You can modify the email template to provide recertification notices to participants. The recertification email table contains the list of templates that can be used for notification of rejected recertification. The table, which can be sorted, contains **Select**, **Name** (such as Delete Access or Remove Account), and **Subject** columns.

The Rejection email template can be customized to provide rejection notices to participants. The Rejection email table contains the list of templates that can be used for notification of rejected recertification. The table, which can be sorted, contains **Select**, **Name** (such as Delete Access or Remove Account), and **Subject** columns.

Note: You can also create your own template. The default templates cannot be modified, but they can be copied to use as the starting point for a new template.

Scheduling options

You can configure a schedule to specify the frequency at which recertification occurs.

You can use the following scheduling options when creating a recertification policy:

- Calendar option
- Rolling option

Calendar option

Use the calendar option to set the schedule for the policy evaluation period. Recertification for all users, accounts and accesses that are targeted by the given policy then occur at the same time. If the setting is monthly on the first day of the month, and the policy targets a service, the recertification policy workflow is triggered on all accounts on that service at the first of every month.

You can use the following types of options:

Daily Recertifies targets every day.

Hourly
Specify the minute of the hour.

Weekly
Specify the day of the week.

Monthly
Specify the day of the month (1-28).

Quarterly
Specify the day of the quarter (1-90).

Annually
Specify the month and day (for example, Jan 28).

Semi-annually
Specify the day (1-180).

During a specific month
Specify the month and day of week or daily and set at a specific time, for example, 12:00 AM.

After specifying the policy evaluation period, you must set the time at which the recertification policy workflow is to be run (for example, 12:00 AM).

Rolling option

You can set the rolling option to ensure that only those targets that have not been recertified within a specified interval are subject to recertification when the policy is evaluated. For example, if an account policy is scheduled for weekly evaluation with a rolling interval of 90 days, only the accounts that were recertified more than 90 days prior are subject to recertification each week. The rolling option is not available for access recertification.

A rolling schedule and calendar schedule are identical in terms of how often the recertification policy is evaluated. The difference is that a calendar schedule always triggers recertification for the target resources when the policy evaluates. A rolling schedule, however, triggers recertification only for the target resources that have not been recertified within the specified interval when the policy evaluates.

Recertification policy results

Depending on the user response, a recertification policy can mark an account, access, group membership, or role membership as recertified. The recertification policy can also suspend or delete the resource or membership.

Recertification states for accounts and accesses

After an activity is completed, an account or access can be in one of the following states:

Active The account or access target is marked as recertified, and no further action is taken. It is not suspended or deleted. If approved, the target remains active, and the entry of the owner is updated.

Marked
The workflow marks the account or access as not certified and issues a rejection notification. The contents of the rejection notification are configured in the policy definition.

Suspended
The workflow suspends the account or access and issues suspension notifications. `Suspended` is not an option for access recertifications because an access cannot be suspended.

Deleted
The workflow deletes the target type and issues rejection notifications.

Note: Audit records are created for each of these actions. The records can be read with the Recertification Change History report. Recertification status for accounts and access entitlements can also be seen with the Account Recertification Status or Access Recertification Status pages.

Recertification states for group membership and role membership

After a recertification activity is completed, a role membership or group membership can be in one of the following states:

Active The membership is marked as recertified, and no further action is taken.

Marked
The membership is marked as not certified, and a rejection notification is sent according to the policy configuration.

Removed
The user is removed from the role, or the account is removed from the group. A rejection notice is sent according to the policy configuration.

Overrides

You can use recertification override tasks to update the recertification status of specific targets without re-evaluating an entire recertification policy.

The **Account Recertification Status** task allows authorized users to manually mark accounts on a service as Recertified. The task applies to owned accounts that are not already recertified. Overriding the recertification status of a suspended account changes the recertification status of the account to Recertified, but it does not restore the account. Authorization for the task is governed by the Recertification Override ACI operation on the service protection category.

To override the recertification status of accounts on a service, navigate to **Manage Services > Select a Service**. Click the icon next to the service name and select **Account Recertification Status** to get to the status page. On the status page, select the accounts to override and click the **Recertify** button. You must enter a justification before recertifying. The justification that you provide for the override is recorded in the audit record and is included in the Recertification Change History report.

The **Access Recertification Status** task allows authorized users to manually mark accesses on a service as Recertified. The task applies to accesses that are not already recertified. Authorization for the task is governed by the Recertification Override ACI operation on the service group protection category.

To override the recertification status of accesses on a service, navigate to **Manage Groups > Select a Service**. Select the service and click **OK**. Then, click the icon next to the group for the accesses and select **Access Recertification Status** to get to the status page. On the status page, select the accesses and click the **Recertify** button. You must enter a justification before recertifying. The justification that you provide for the override is recorded in the audit record and is included in the Recertification Change History report.

The **Recertify** task allows system administrators to trigger a user recertification activity for a specific user and policy.

Creating an account recertification policy

As an administrator, you can create an account recertification policy to use with one or more services or access instances. For example, you might create a recertification policy that specifies that managers must recertify their employee accounts every 60 days.

Before you begin

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

Before you create a recertification policy, one or more service instances must exist.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Recertification Policies**.
2. On the Recertification Policies page, in the **Recertification Policies** table, click **Create**.
3. On the Manage Recertification Policies page, on the General page, complete these steps:
   a. Type a name for the recertification policy.
   b. Optional: Type a description for the recertification policy.
   c. Select the status of the policy, enabled or disabled.
   d. Select the business unit to which the policy applies
   e. Select the scope of the business unit that you selected.
   f. Click **Next**.
4. On the Target Type page, select **Accounts**, and then click **Next**.
5. On the Service Target page, add one or more specific services to associate with the policy, and then click **Next**.
6. To add one or more services:
   a. Click **Add**.
   b. On the Services page, type your search criteria, and then click **Search**.
   c. In the Services table, select one or more services.
   d. Click **OK**.
7. On the Schedule page, select the schedule type and evaluation frequency, and then click **Next**.
8. On the Policy page, select either simple or advanced configuration mode, and then click **Next**. If you choose the advanced mode, use the workflow designer to configure the policy.

   Note: On the Policy page, you can also specify the following options:
   - Who approves recertification
   - The action, such as suspend or delete, that occurs when a participant declines to recertify an account
   - An optional recipient who receives the rejection email, which can be configured to none, such as a manager, who is notified when recertification is declined
   - A value for the number of days in which the participant must respond to the recertification request
   - An action, such as reject or approve, that occurs when the recertification response interval expires
   - A user type to specify the scope of the recertification policy to apply only to people of a certain type on the specified policy schedule

Note: The user type option includes a performance penalty for using options other than `all`. If the person or business partner (bp) person type is chosen, IBM Security Identity Manager still retrieves all accounts from the LDAP server. IBM Security Identity Manager then iterates through the accounts, does an LDAP search to look up owners of the accounts, and determines if the owner is of the type `person` or `bp person`. If your user population is large, doing two searches per account can be expensive.

9. On the Recertification E-mail page, select an email template, and click **Next**.
10. On the Rejection E-mail page, select a rejection email template, and click **Finish**.
11. On the Success page, click **Close**.

Creating an access recertification policy

As an administrator, you can create an access recertification policy for use with one or more access instances.

Before you begin

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

About this task

Before you create a recertification policy, an access instance must exist.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Recertification Policies**.
2. On the Recertification Policies page, in the **Recertification Policies** table, click **Create**.
3. On the Manage Recertification Policies page, on the General page, complete these steps:
   a. Type a name for the recertification policy.
   b. Optional: Type a description for the recertification policy.
   c. Select the status of the policy, enabled or disabled.
   d. Select the business unit to which the policy applies
   e. Select the scope of the business unit that you selected.
   f. Click **Next**.
4. On the Target Type page, select **Access**, and then click **Next**.
5. On the Access Target page, add one or more specific accesses to associate with the policy, and then click **Next**.
6. To add one or more accesses, complete these steps:
   a. Click **Add**.
   b. On the Accesses page, type your search criteria, and then click **Search**.
   c. In the **Accesses** table, select one or more accesses.
   d. Click **OK**.
7. On the Schedule page, select the schedule type and evaluation frequency, and then click **Next**.

8. On the Policy page, select the configuration mode, and then click **Next**. If you choose the advanced mode, use the workflow designer to configure the policy.

   Note: On the Policy page, you can also specify the following options:
   - Who approves recertification
   - The action, such as suspend or delete, that occurs when a participant declines to recertify an access
   - An optional recipient who receives the rejection email, which can be configured to `none`), such as a manager, who is notified when recertification is declined
   - A value for the number of days in which the participant must respond to the recertification request
   - An action, such as reject or approve, that occurs when the recertification response interval expires
   - A user type to specify the scope of the recertification policy to apply only to people of a certain type on the specified policy schedule

     Note: The user type option includes a performance penalty for using options other than `all`. If the person or business partner (bp) type is chosen, IBM Security Identity Manager still retrieves all accounts from the LDAP server. IBM Security Identity Manager then iterates through the accounts, does an LDAP search to look up the owners of the accounts, and determines if the owner is of the type `person` or `bp person`. If your user population is large, doing two searches per account can be expensive.
9. On the Recertification E-mail page, select an e-mail template, and then click **Next**.
10. On the Rejection E-mail page, select a rejection e-mail template, and then click **Finish**.
11. On the Success page, click **Close**.

Creating a user recertification policy

As an administrator, you can create a user recertification policy to recertify the accounts, group membership of accounts, and memberships of users.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Recertification Policies**.
2. On the Recertification Policies page, in the **Recertification Policies** table, click **Create**.
3. On the Manage Recertification Policies page, on the General page, complete these steps:
   a. Type a name for the recertification policy.
   b. Optional: Type a description for the recertification policy.
   c. Select the status of the policy, enabled or disabled.
   d. Select the business unit to which the policy applies.

e. Select the scope of the business unit that you selected.
f. Click **Next**.

4. On the Target Type page, select **Users**, and then click **Next**.
5. On the User Target page, select the user type, and then click **Next**.
6. On the Resource Target page, complete these steps:
   a. Select which roles you want the policy to recertify membership on.
   b. Select which accounts you want the policy to recertify.
   c. Select which groups you want the policy to recertify.
   d. Click **Next**.
7. Optional: If you selected **Specified roles** on the Resource Target page, on the Role Target page, select one or more roles for which you want to recertify membership.
8. Optional: If you selected **Accounts on specified services** on the Resource Target page, on the Account Target page, select one or more services for which accounts on the service are recertified.
9. Optional: If you selected **Specified groups** on the Resource Target page, on the Group Target page, select one or more groups you want the policy to recertify.
10. On the Schedule page, select the schedule type and evaluation frequency, and then click **Next**.
11. On the Policy page, select the configuration mode, and then click **Next**. If you choose the advanced mode, use the workflow designer to configure the policy.

    Note: On the Policy page, you can also specify the following options:
    - Who approves recertification.
    - An action, such as Suspend accounts and mark others, that occurs when the recertification is rejected.
    - An optional recipient who receives the rejection email (which can be configured to None) such as a manager, who is notified when recertification is declined.
    - A value for the number of days in which the participant must respond to the request until the recertification is due.
    - An action, such as Reject All or Approve All, that occurs when the recertification is overdue. If you do not select an action, the recertification activity remains in the activity list of the participant after the due date until it is completed.
12. On the Recertification E-mail page, select an email template, and then click **Next**.
13. On the Rejection E-mail page, select a rejection email template, and then click **Finish**.
14. On the Success page, click **Close**.

Changing a recertification policy

As an administrator, you can change a recertification policy. For example, you can modify the recertification interval, add or remove users, services, or access instances. Alternatively, you can modify the template that provides a message when recertification is declined.

Before you begin

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

About this task

If you modify a recertification policy, ensure that you consider the consequences of the changes. For example, when the schedule for recertification is modified, the changes might require users, accounts, or accesses that were recently recertified to be recertified again immediately. When setting the default timeout action, ensure that you properly set up the participant of recertification. An escalation participant is not specified in the default simple workflow.

Suppose that a recertification policy exists for LDAP accounts and the notifications for recertification are sent to all account owners. If the target for the recertification policy is changed from LDAP service to Win local service, the LDAP accounts still must be recertified by the LDAP account owners. Because the to-do activities for LDAP recertification are already created, the timeout action and the action upon rejection are applicable as specified in the LDAP recertification policy before updating. To-do items that are already in process are not deleted automatically, and progress to their natural ending.

You can use policy modification to *disable* a policy. If you disable a policy, the policy does not generate any additional recertification to-do items until it is re-enabled. However, any running recertifications are not stopped, and they complete as normal.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Recertification Policies**.
2. On the Recertification Policies page, type information about the recertification policy or service in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and then click **Search**.
3. In the **Recertification Policies** table, locate and select a recertification policy that you want to change, and then click **Change**.
4. On the Manage Recertification Policies page, modify the information on the available pages.
5. Click **OK** to save the changes.
6. On the Success page, click **Close**.

Deleting a recertification policy

As an administrator, you can delete a recertification policy that is no longer needed to manage user, account, or access recertification.

Before you begin

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

About this task

If you delete the recertification policy, any users, accounts, or accesses that were targeted by that policy are no longer governed by any recertification policy.

Suppose that a recertification policy exists for LDAP accounts and the notifications for recertification are sent to all account owners. If the policy is deleted, the LDAP accounts still must be recertified by LDAP account owners. Because the to-do activities for LDAP recertification are already created, the timeout action and action upon rejection are applicable as specified in the LDAP recertification policy before deletion.

However, any running recertifications are not stopped, and they complete as normal.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Recertification Policies**.
2. On the Recertification Policies page, type information about the recertification policy or service in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and then click **Search**.
3. In the **Recertification Policies** table, locate and select a recertification policy that you want to delete and click **Delete**.
4. On the Confirmation page, review the recertification policy that you want to delete and click **Delete**.
5. On the Success page, click **Close**.

Recertification default notifications

IBM Security Identity Manager provides default templates for user, account, and access recertification notifications.

Default recertification templates

The default templates exist in LDAP and cannot be modified. An administrator can view the default templates in the recertification policy interface and copy them there.

The following labels are the default template names for the account and access recertification policy recertification email:

- Delete Account
- Mark Access
- Mark Account
- Remove Access
- Suspend Account

The following labels are the default template names for the account and access recertification policy rejection email:

- Access Marked
- Access Removed
- Account Deleted
- Account Marked
- Account Suspended

The following labels are the default template names for the user recertification policy recertification e-mail:

- User Recertification Pending

The following labels are the default template names for the user recertification policy rejection e-mail:

- User Recertification Rejected

Properties file values

To change templates, you can use all the key=value statements in the `CustomLabels.properties` file, or create your own properties and values.

These properties are referenced by the default templates. The properties can be modified if you want to reword some of the templates while keeping the same parameter substitutions. You can either modify these defaults, or make up your own keys and reference them from the templates.

The properties include the following items on one line:

```
recertOn={0} on {1}
recertTemplateSubject=Recertification required
  for account {0} on service {1}
recertTemplateAccessSubject=Recertification required
  for account {0} on access {1}
recertTemplateBody=You have received a recertification request
  for account {0} on service {1} owned by {2}.
recertTemplateAccessBody=You have received a recertification request
  for account {0} on access {1} owned by {2}.
recertDeclineSuspendsBody=Rejection of this recertification request
  will result in the suspension of account {0} on {1}.
recertDeclineDeletesBody=Rejection of this recertification request
  will result in the deletion of account {0} on {1}.
recertDeclineMarksBody=Rejection of this recertification request
  will result in account {0} on {1} being marked as rejected for
  recertification.
recertDeclineDeletesAccessBody=Rejection of this recertification
  request will result in the deletion of access {0}.
recertDeclineMarksAccessBody=Rejection of this recertification request
  will result in access {0} being marked as rejected for recertification.
recertDeclinedAcctSuspendedSubj=Account {0} on service {1} has been
  suspended due to rejection of a recertification request
recertDeclinedAcctDeletedSubj=Account {0} on service {1} has been
  deleted due to rejection of a recertification request
recertDeclinedAcctMarkedSubj=Account {0} on service {1} has been
  marked as rejected for recertification due to rejection
  of a recertification request
recertDeclinedAccessDeletedSubj=Account {0} on access {1} has been
  deleted due to rejection of a recertification request
recertDeclinedAccessMarkedSubj=Account {0} on access {1} has been
  marked as rejected for recertification due to rejection of a
  recertification request
recertDeclinedAcctSuspendedBody=The account {0} on service {1} owned
  by {2} has been suspended due to rejection of a recertification request.
recertDeclinedAcctDeletedBody=The account {0} on service {1} owned
  by {2} has been deleted due to rejection of a recertification request.
recertDeclinedAcctMarkedBody=The account {0} on service {1} owned
  by {2} has been marked as rejected for recertification due to
  rejection of a recertification request.
recertDeclinedAccessDeletedBody=The account {0} on access {1} owned
  by {2} has been deleted due to rejection of a recertification request.
recertDeclinedAccessMarkedBody=The account {0} on access {1} owned
  by {2} has been marked as rejected for recertification due to
```

```
  rejection of a recertification request.
userRecertTemplateSubject=Recertification required for user {0}
userRecertTemplateBody=You have received a recertification request
  for user {0}. The recertification includes their membership in {1} role(s)
  and ownership of {2} account(s). Please indicate whether the user still
  requires these resources.
userRecertDeclinedSubj=Recertification request rejected for user {0}
userRecertDeclinedBody=One or more resources for user {0} have been
  rejected during recertification.
userRecertRolesRejectedLabel=The following roles were rejected:
userRecertAccountsRejectedLabel=The following accounts were rejected,
  along with all groups associated with the accounts:
userRecertGroupsRejectedLabel=The following groups were rejected,
  but the account was accepted:
userRecertAcctLabel=Account "{0}" on service "{1}"
userRecertGroupLabel=Group "{0}" for account "{1}" on service "{2}"
```

Separation of duty policies

A *separation of duty policy* is a logical container of separation rules that define mutually exclusive relationships among roles. Policies for separation of duty are defined by one or more business rules. The rules exclude users from membership in multiple roles that might present a business conflict.

A separation of duty policy uses business rules to define the relationships among roles. The separation of duty policy groups the business rules for ease of administration. For example, you can assign a set of administrators to a policy, making the administrators responsible for tracking the violations of a set of rules.

Policy owners

You can specify one or more owners for the policy. Owners can be any combination of users and roles. You can configure policy owners to participate in policy and role change workflows. For example, a policy owner can approve or reject separation of duty violation activities that occur when roles are added to a Security Identity Manager user. Separation of duty policy owners can also:

- Exempt users or revoke exemptions from any policy violations that occur
- Be used as principals in system access control items (ACIs)

Exemption approval and revocation

Policy owners can approve and revoke exemptions by default, but they do not necessarily require this ability. You can configure roles or users to have access control capabilities over separation of duty policies though ACIs. The ACIs allow policy owners to do tasks such as editing or tracking violations. You can also configure the approval workflow to use participants other than the policy owner.

Separation of duty rules

A separation of duty policy can include multiple rules. For each rule, two or more roles must be listed. The number of roles to which a user can belong depends on how many roles you allow in the rule. The number of roles that you allow to coexist must be one fewer than the total number of roles in the list. For example, you might create a rule that excludes procurement and order approval. The allowed number of roles in the rule must be one, meaning that a user can have only one role. If you add more roles, such as invoicing and financing, you can allow up to three roles. Each user can have three different roles and the system capabilities defined by that role.

Allowed roles set to greater than one are typically used to prevent one person from having complete control over a process. The process is described by a set of roles. For example, a rule named "A user cannot have full control over the procurement process" might be defined by three roles named purchaser, approver, and orderer. In this example, the rule has two allowed roles. A user can be a member of two of these roles, but the user cannot a member of all three roles.

Enabled and disabled policies

An *enabled policy* creates exemption approvals and warns users before they submit a role membership change that breaks a separation of duty rule.

A *disabled policy* can still track violations, but it does not generate approvals or warn users. Violations from disabled policies are not displayed in audit reports. Using a disabled policy is a good way for a security administrator to track violations that occur before a policy is active in the system.

Role hierarchy and rules

Two roles in a rule cannot be direct ascendants or descendants of each other in the role hierarchy. For example, you cannot have a rule with both HR organization and HR department *x* if HR department *x* is a child role of HR organization.

ACI operations for the separation of duty policy protection category

You can configure role owners to have access control capabilities over separation of duty policies though access control items (ACIs). The ACIs allow role owners to do tasks such as editing or tracking violations. ACIs must apply to the business unit in which the policy is defined. Creators of separation of duty ACIs can define ACI filter rules to scope the policies to which an ACI applies.

Add Protects separation of duty policy creation. The add operation fails if this ACI is not met.

Exemption Administration
Protects separation of duty policy violation and exemption management through the Violations and Exemptions Summary page. The ability to exempt a violation or revoke an exemption is governed by this operation. The **Approve** and **Revoke** buttons are not displayed if this ACI is not met. The operations of exempt and revoke also apply to the public API.

Modify
Protects separation of duty policy modifications. The modify operation fails if this ACI is not met. When change is denied and search is allowed, the user has a read-only view of the policy.

Reconcile
Protects separation of duty policy reconciliation. Separation of duty policy reconciliation is the operation that analyzes the policy separations and creates violations or cleans up violations or exemptions. Clicking the **Evaluate** button causes a "not authorized" message to be displayed if this ACI is not met.

Remove
Protects separation of duty policy deletions. Clicking the **Delete** button causes a "not authorized" message to be displayed if this ACI is not met.

Search
Protects separation of duty policy searches. With the search operation granted, the user can see details about violations and exemptions. If a user is authorized for search but not modify, the user can open the policy in a read-only mode and view violations and exemptions. However, the user cannot act on those violations and exemptions or change the policy.

Default ACIs for the separation of duty policy

See descriptions of the default access control items (ACIs) for separation of duty capabilities.

Grant Search to Auditor Group
Allows the auditor group to view the policies, rules, violations, and exemptions.

Grant All to Owner
Grants all operations to the owner of a separation of duty policy in the organization. You might allow a user who is not a system administrator to create a separation of duty policy. You must create an ACI that grants the **add** permission to that user.

Separation of duty approval workflow operation

After you create the policy, an approval workflow operation named *approveSoDViolation* for each violation is started during person operations. These operations might be role membership changes that cause separation of duty policy violations.

There is one separation of duty approval workflow that is called for all separation of duty violations. However, you can customize the workflow for individual policies to have multilevel approval, but the customizations must be done from within that one workflow.

To locate the *approveSoDViolation* approval operation, click **Configure System > Manage Operations**, and then select **Global level**. The approval operation is called for each violation that is found during the person operation (role membership change). You can modify this operation to include custom approval paths. For example, you can specify that both the policy owner and the user's manager approve the violation. By default, the policy owner is the approval participant. This image illustrates the *approveSoDViolation* approval operation.

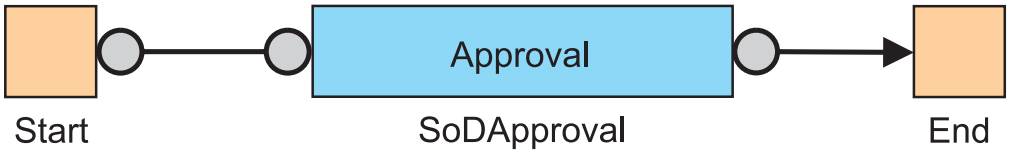


Figure 2. `approveSoDViolation` approval operation

After the approval participant approves the operation, the person operation is allowed to occur (implying approved) or fail (implying the approval was rejected). During the approval path, a violation exemption is recorded, noting who approved the exemption. The violation and exemption statistics are updated. You can view the exemption by clicking **Manage Policies > Manage Separation of Duty Policies**, and then clicking a number in the **Exemptions** column of the **Separation of Duty Policies** table.

When you request a change, such as adding a role to a user, a warning might be displayed. The warning indicates that the change can cause a separation of duty violation. The warning lists the policy and rule in violation. You can continue to submit the request or cancel the request. The warning is displayed in both the administrative console and the Self Service or the Identity Service Center interface for the following requests:

- Modifying or creating a person
- Requesting an access
- Modifying static role membership
- Changing the role hierarchy

If you try to change role hierarchy in such a way that an existing separation of duty policy would become invalid, an error is displayed. The change does not occur. The error lists the policy and rule that would be in violation if the role hierarchy was modified as requested.

The audits of the exemption process occur automatically, depending on the result of the workflow. You do not need to manually call audit methods to have the audits recorded for use in the administrative console or reports.

However, you must set the process result with `AA` and process result detail with the string value that you want to audit as the justification for the exemption approval if the intent is to allow the violation to exist in the system. By default, the approval operation in the *approveSoDViolation* workflow has this PostScript code:

```
WorkflowRuntimeContext.setProcessResult(WorkflowRuntimeContext.getActivityResult());
WorkflowRuntimeContext.setProcessResultDetail(WorkflowRuntimeContext.getActivityResultDetail());
```

The first line in the PostScript code sets the process result to the same value as the result of the approval. `AA` indicates approved and `AR` indicates rejected. The second line sets the process result detail to the comments that were typed by the user when the approval to do activity was approved.

You can use normal workflow customizations to get the values you want, but be sure to call `WorkflowRuntimeContext.setProcessResult()` and `WorkflowRuntimeContext.setProcessResultDetail()` with some value if you want the system to treat the approval as an approved separation of duty exemption.

There might be multiple approvals in the workflow for separation of duty. The approver that is listed in the exemption record is the last person to approve an approval request in the workflow.

Separation of duty policy violations and exemptions

A *violation* is a specific violation of a separation of duty policy, and an *exemption* is an approved separation of duty violation. *Policy evaluation* is a way to discover violations.

Policy violations

A *violation* is a specific violation of a separation of duty policy, which means that the roles for a user have a conflict that is based on a defined separation of duty rule.

Violations are created when the following events occur:

- A user requests membership in a role that would violate one or more separation of duty policy rules.
- A user creates a separation of duty policy or rule.
- User records are fed into Security Identity Manager through an identity feed if they create a rule violation.
- Any other request to modify role membership if it creates a rule violation.
- When there are existing conflicts when a policy is introduced.
- A security administrator revokes an exemption.

When a policy is created or changed, the violations do not update automatically. You must either perform an evaluation on the policy or wait for a scheduled data synchronization.

Policy exemptions

An *exemption* is an approved separation of duty violation, which means that the conflict cannot be flagged as a violation in an audit, and additional updates to the user's role list do not require reapproval. Exemptions occur when a security administrator approves a request that violates a defined and active separation of duty policy. A security administrator can also convert existing violations into exemptions.

Exemptions are created for a specific policy rule, not for an entire policy. If a policy contains multiple rules and the user is approved for the violation of one rule, that user is not automatically allowed to violate the other rules in the policy.

Exemptions remain stored in the database when a policy is disabled. Therefore, if a policy is disabled and then re-enabled at a later date, the exemptions are remembered.

You can exempt a user from violating separation of duty policy rules manually or through an approval process.

When a rule violation event occurs and a policy and role change workflow activity have been defined, an approval activity is created for workflow participants (such as policy owners) to exempt the user from a specified separation of duty policy rule. Only a role membership change request for the user triggers an approval activity.

An approval activity is generated for each rule violation. If the approval is rejected, any modifications to the user that were made at the time of the role membership change are lost. If an exemption approval request is triggered as part of a person being created, that person is not created if the approval is rejected.

Policy evaluation

Policy evaluation is a way to discover violations, and can occur in any of these situations:

- Use the **Evaluate** button. This button causes the policy to be evaluated against all people who currently have roles in the policy.
- Perform a data synchronization. Rule violations are recorded for each policy, and the number of violations is displayed in the separation of duty policy table. You can then exempt any rule violations manually by clicking the link provided in the table and viewing or modifying any rule violations and exemptions.

- When you create any HR feed service, you can specify whether to evaluate the separation of duty policy. If you choose to evaluate the separation of duty policy, you must also enable workflow. If this option is enabled, an approval activity is generated for each separation of duty rule violation that is found in the incoming HR feed data. That approval process must be marked as approved to get the updates into Security Identity Manager. If the approval processes are rejected, the entire entry or change that was in that HR feed record is ignored and is not stored in Security Identity Manager.

Enabling the Manage Separation of Duty Policies portfolio task

System administrators have access to the Manage Separation of Duty Policies portfolio task. Other users must be assigned to a group that has access to the task.

Before you begin

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

About this task

To have the **Manage Separation of Duty Policies** portfolio task be displayed in the administrative console, you must enable the task in one of the default views or in a view that you created.

To enable the **Manage Separation of Duty Policies** portfolio task, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security** > **Manage Views**. The Define Views page is displayed.
2. On the Define Views page, complete these steps:
   a. In the **Name** field, type information about the view and click **Search**. The **Manage Views Results** table is displayed.
   b. In the **Manage Views Results** table, select the check box next to a view and click **Change**.
   c. Optional: In **General** tab, change the name or description of the view.
   d. In the **Configure View** tab, in the tree of tasks, expand **Manage Policies**, and then select **Manage Separation of Duty Policies** task. Both **Manage Policies** and **Manage Separation of Duty Policies** are selected.
   e. Click **OK** to save the changes.

Results

A Success page is displayed, indicating that you successfully updated the views on the system.

What to do next

You can continue working with views, or click **Close**.

Creating separation of duty policies

An administrator can create a separation of duty policy to use for auditing purposes. For example, you might create a separation of duty policy to report users that belong to multiple roles that are mutually exclusive.

Before you begin

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

To create a valid policy rule, you must have two or more roles defined in the system for the business unit you select.

About this task

To create a separation of duty policy, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Separation of Duty Policies**. The Manage Separation of Duty Policies page is displayed.
2. On the Manage Separation of Duty Policies page, in the **Separation of Duty Policies** table, click **Create**. The Create a Separation of Duty Policy page is displayed.
3. On the Create a Separation of Duty Policy page, complete these steps:
   a. Type a name for the policy.
   b. Provide a description for the policy.
   c. Select the business unit to which this policy applies. Click **Search** to search for a business unit. The Business Unit page is displayed.
4. On the Business Unit page, complete these steps:
   a. Type your search criteria, and then click **Search**.
   b. In the **Business Units Found** table, select a business unit and click **OK**. The Create a Separation of Duty Policy page is displayed.
5. On the Create a Separation of Duty Policy page, in the **Policy Rules** table, click **Create**. The Create Policy Rule page is displayed.
6. On the Create Policy Rule page, complete these steps:
   a. In the **Description of separation** field, type a description for the policy rule. For example, you might describe a rule that you add to a policy as `People in the IT department may not be given accounting responsibilities`.
   b. Type each role name that you want to add to the role separation list and click **Add**. If you type the exact name of an existing role in the **Role name** field and click **Add**, the role is immediately added to the list. If you type a value in the **Role name** field that does not exactly match a role or matches more than one role, a search panel opens. Select the appropriate roles.

      Note: You can search only for the roles for which you have permission.
   c. In the **Allowed number of roles** list, select the number of roles to which a user can belong. For each policy rule that you create, two or more roles must be listed. The number of roles to which a user can belong depends on how many roles you allow in the policy rule. The number of roles that you allow can be, at a maximum, one fewer than the total number of roles in the list.

d. Click **OK**. The Create a Separation of Duty Policy is displayed.

7. On the Create a Separation of Duty Policy page, complete these steps:
   a. Create more policy rules as necessary.
   b. Click the icon next to **Policy Owners**. The **Role Policy Owners** table and the **User Policy Owners** table are displayed.
   c. In the **Role Policy Owners** table, click **Add** to search for and select roles to have ownership of the policy.
   d. In the **User Policy Owners** table, click **Add** to search for and select users to have ownership of the policy.
   e. In the **Policy state** field, select whether to enable or disable the policy. An *enabled policy* creates exemption approvals and warns users before they submit a role membership change that breaks a separation of duty rule. A *disabled policy* can still track violations, but it does not generate approvals or warn users. Violations from disabled policies are not displayed in audit reports. Using a disabled policy is a good way for a security administrator to track violations that occur before a policy is active in the system.
   f. Click **Submit** to save the policy.

Results

A Success page is displayed, indicating that you successfully submitted a request for a new separation of duty policy.

What to do next

You can view your request, continue working with policies, or click **Close**.

Modifying separation of duty policies

An administrator can modify a separation of duty policy. For example, you can add or remove policy owners. You can also add or remove separation rules, change role attributes for a specific rule, and enable or disable the policy.

Before you begin

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

About this task

You can use policy modification to disable or enable a policy. If you disable a policy, the policy does not generate any additional to-do items until you re-enable it.

You cannot change the business unit to which the policy applies.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Separation of Duty Policies**. The Manage Separation of Duty Policies page is displayed.
2. On the Manage Separation of Duty Policies page, complete these steps:
   a. Type information about the policy in the **Search information** field.

b. In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**. A list of policies that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

c. In the **Separation of Duty Policies** table, select the check box next to the policy that you want to modify, and then click **Change**. Selecting the check box at the top of this column selects all policies. The Change Separation of Duty Policy page is displayed.

3. On the Change a Separation of Duty Policy page, complete these steps:
   a. Provide any necessary updates to the policy name and description.
   b. In the **Policy Rules** table, create, delete, or modify any rules that apply to the policy.
   c. Click the icon next to **Policy Owners**. The **Role Policy Owners** table and the **User Policy Owners** table are displayed.
   d. Optional: In the **Role Policy Owners** table, click **Add** to search for and select roles to have ownership of the policy.
   e. Optional: In the **User Policy Owners** table, click **Add** to search for and select users to have ownership of the policy.
   f. Select whether to enable or disable the policy.
   g. Click **Submit** to save the policy.

Results

A Success page is displayed, indicating that you submitted a request to change a separation of duty policy.

What to do next

You can continue working with separation of duty policies, view your request, or click **Close**.

Evaluating separation of duty policies

An administrator can evaluate a separation of duty policy without doing a data synchronization. By running the evaluation, you can view current policy violation and exemption information. The evaluation process searches for violations to the policies that you specify.

Before you begin

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

About this task

Violations are kept current as user role membership is modified. There are some cases where a change in the system might require a re-evaluation of separation of duty policy violations for one or more specific policies. These situations include:

- Creating or changing a separation of duty policy
- Changing a role hierarchy

- Running an identity feed with evaluations disabled

In these cases, run a separation of duty policy violation evaluation on one or more policies. You can do the evaluation in one of these ways:

- By running a full report data synchronization, which finds violations for all policies
- By running evaluations on individual policies

When you disable a policy and then do another evaluation on the disabled policy, new violation warnings or exemption approval to-do activities are generated.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Separation of Duty Policies**. The Manage Separation of Duty Policies page is displayed.
2. On the Manage Separation of Duty Policies page, complete these steps:
   a. Type information about the policy in the **Search information** field.
   b. In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**. A list of policies that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Separation of Duty Policies** table, select the check box next to the policy that you want to evaluate, and then click **Evaluate**. Selecting the check box at the top of this column selects all policies. A confirmation page is displayed.
   d. On the Confirm page, click **Evaluate** to run the evaluation, or click **Cancel**.

Results

A Success page is displayed, indicating that you successfully submitted a request to do an evaluation on a separation of duty policy.

After the evaluation is complete, the violation count for the policy is updated.

What to do next

You can continue working with separation of duty policies, view your request, or click **Close**.

Deleting separation of duty policies

As an administrator, you can delete a separation of duty policy that is no longer needed to manage exclusive relationships between roles.

Before you begin

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

About this task

If you delete the separation of duty policy, any roles that were targeted by that policy are no longer governed by the separation of duty policy.

When you delete a policy, all violations and exemptions for that policy are retained and marked with a statement that the policy is deleted.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Separation of Duty Policies**. The Manage Separation of Duty Policies page is displayed.
2. On the Manage Separation of Duty Policies page, complete these steps:
   a. Type information about the policy in the **Search information** field.
   b. In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**. A list of policies that match the search criteria is displayed.

      If the table contains multiple pages, you can:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Separation of Duty Policies** table, select the check box next to the policy that you want to delete, and then click **Delete**. Selecting the check box at the top of this column selects all policies. A confirmation page is displayed.
3. On the Confirm page, click **Delete**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted the policy for deletion.

What to do next

Continue working with policies, view your request to confirm that the policy is deleted, or click **Close**.

Viewing policy violations and exemptions

An administrator or policy owner can view a summary of the separation of duty policy violations and exemptions for each rule in the policy. The administrator or policy owner can also do administrative operations, such as approve or revoke, on the violations and exemptions.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Separation of Duty Policies**. The Manage Separation of Duty Policies page is displayed.
2. On the Manage Separation of Duty Policies page, complete these steps:
   a. Type information about the policy in the **Search information** field.

b. In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**. A list of policies that match the search criteria is displayed.

   If the table contains multiple pages, you can:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

c. In the **Separation of Duty Policies** table, click the link provided in the **Violations** or **Exemptions** column of the policy that you want to view. The link is displayed only if there are one or more violations or exemptions for the separation of duty policy. The Violations and Exemptions Summary page is displayed.

3. On the Violations and Exemptions Summary page, complete these steps:
   a. Select the order in which you want to sort the rules, and then click **Sort**. You can sort alphabetically by rule name, or sort by the number of violations or exemptions.
   b. Click the icon (▸) next to each rule that you want to view, or click the rule name.

Results

Two tables that provide information about violations and exemptions are displayed.

What to do next

You can approve violations or revoke exemptions.

When you are done viewing violations and exemptions, click **Close**.

Approving policy violations

An administrator or policy owner can approve separation of duty policy violations for each rule in the policy.

Before you begin

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

About this task

When you approve a violation, an exemption is created for the specified user and the combination of roles that caused the violation. After you approve a policy violation, that violation is removed from the violation list, and a new exemption is displayed in the exemption list.

Having an exemption means that the user is allowed to be a member of the violating roles. Updates to the user's person record do not cause additional violations or warnings unless the user introduces a new violation that is not covered by the exemption.

Updates to the record of a person do not trigger an approval unless the roles of the person are updated and the combination violates a separation of duty policy, assuming that an exemption does not exist for the policy.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Separation of Duty Policies**. The Manage Separation of Duty Policies page is displayed.
2. On the Manage Separation of Duty Policies page, complete these steps:
   a. Type information about the policy in the **Search information** field.
   b. In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**. A list of policies that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Separation of Duty Policies** table, click the link provided in the **Violations** column of the policy that you want to view. The link is displayed only if there are one or more violations for the separation of duty policy. The Violations and Exemptions Summary page is displayed.
3. On the Violations and Exemptions Summary page, complete these steps:
   a. Select the order in which you want to sort the rules, and then click **Sort**. You can sort alphabetically by rule name, or sort by the number of violations or exemptions.
   b. Click the icon (▸) next to each rule that you want to view. The **Violations** table is displayed, providing information about violations for the rule that you specified.
   c. In the **Violations** table, select the check box next to one or more violations that you want to approve, and then click **Approve**. Selecting the check box at the top of this column selects all violations. The Approve Violations page is displayed.
4. On the Approve Violations page, complete these steps:
   a. In the **Violation Summary**, ensure that the policies and rules are correct.
   b. In the **Notes** field, type a reason for approving the violation, and then click **Approve**.

Results

A Success page is displayed, indicating that you successfully approved the violations for the specified policy and rule.

What to do next

You can approve additional violations or revoke exemptions.

When you are done viewing violations and exemptions, click **Close**.

Revoking policy exemptions

An administrator or policy owner can revoke separation of duty policy exemptions for each rule in the policy.

Before you begin

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

About this task

When you revoke an exemption, that exemption is removed from the exemption list. The user to which the exemption applies might continue to have roles that are in violation of a separation of duty policy rule. In that case, the violation is displayed again the list of violations for that policy.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Separation of Duty Policies**. The Manage Separation of Duty Policies page is displayed.
2. On the Manage Separation of Duty Policies page, complete these steps:
   a. Type information about the policy in the **Search information** field.
   b. In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**. A list of policies that match the search criteria is displayed.

      If the table contains multiple pages, you can:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c. In the **Separation of Duty Policies** table, click the link provided in the **Exemptions** column of the policy that you want to view. The link is displayed only if there are one or more exemptions for the separation of duty policy. The Violations and Exemptions Summary page is displayed.
3. On the Violations and Exemptions Summary page, complete these steps:
   a. Select the order in which you want to sort the rules, and then click **Sort**. You can sort alphabetically by rule name, or sort by the number of violations or exemptions.
   b. Click the icon (▸) next to each rule that you want to view. The **Exemptions** table is displayed, providing information about exemptions for the rule that you specified.
   c. In the **Exemptions** table, select the check box next to one or more exemptions that you want to revoke, and then click **Revoke**. Selecting the check box at the top of this column selects all exemptions. The Revoke Exemptions page is displayed.
4. On the Revoke Exemptions page, complete these steps:
   a. In the **Exemption Summary**, ensure that the policies and rules are correct.
   b. In the **Notes** field, type a reason for revoking the exemption, and then click **Revoke**. The **Notes** field is for auditing purposes and is not displayed in the administrative console after an exemption is revoked.

Results

A Success page is displayed, indicating that you successfully revoked the exemptions for the specified policy and rule.

What to do next

You can revoke additional exemptions or approve violations.

You can use a custom audit data report to provide justification for revoking exemptions.

When you are done viewing violations and exemptions, click **Close**.

Service selection policies

A *service selection policy* extends provisioning policies by enabling selection of a service based on person attributes. To be enforced, a service selection policy must be the target of a provisioning policy. The service selection policy then identifies the service type to target and defines the service based on JavaScript.

The service selection policy can be in the same container as the provisioning policy or in a container located above the container of the provisioning policy. The scope of a service selection policy determines which provisioning policies can target it. Service selection policies with single scope can be targeted only by provisioning policies at the same level in the organization tree as the service selection policy. Service selection policies with subtree scope can be targeted by provisioning policies at the same level or below the service selection policy.

Service selection policies are evaluated in the following circumstances:

- When a user is added to an organizational role that is a member of a provisioning policy that targets the service selection policy
- When a user's attributes are modified
- When the policy itself is modified

Evaluating the policy might require moving a user's account to a different service instance than the one the user is currently using. A new account for the user is created on the new service instance. One of the following actions completes, depending on the policy enforcement setting of the service instance:

- Suspends the existing user account on the old service instance.

  Note: The account is deleted, suspended, or marked as disallowed only if the service selection policy does not allow the account on that service. An account on the new service is not created.
- Deletes the existing user account on the old service instance.
- Sends a work item to alert the recipient to delete the existing user account on the old service instance.
- Marks the account on the old service instance as disallowed.

Creating a service selection policy

An administrator can create a service selection policy.

Before you begin

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

About this task

A service selection policy is not used by the IBM Security Identity Manager Server until a provisioning policy targets it. If you enable a service selection policy after you enable a provisioning policy, the Security Identity Manager Server does a policy check and uses the policy to provision new and existing accounts.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Service Selection Policies**.
2. On the Work With Service Selection Policies page, in the **Service Selection Policies** table, click **Create**.
3. On the Manage Service Selection Policies page, on the General page, type a name and select a business unit for your service selection policy.
4. Click the **Service Type** tab, and select the type of service you want to associate with the service selection policy.
5. On the Manage Service Selection Policies page, on the Service Selection Script page, type a selection script.

   Important: The Security Identity Manager Server does not verify that the JavaScript is correctly coded. Verify that the JavaScript is correctly coded before using it to define the service selection policy.
6. Click **Submit Now** to save the policy.
7. On the Success page, click **Close**.

Changing a service selection policy

An administrator can change a service selection policy. Service selection policies are not usually modified after being created.

Before you begin

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

About this task

Modifying an existing, enabled service selection policy can cause deprovisioning of user accounts. Modifying the scope or status of a service selection policy can affect user access as soon as the policy changes take effect.

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Service Selection Policies**.
2. On the Work With Service Selection Policies page, type information about the service selection policy or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Service Selection Policies** table, locate and select a service selection policy, and then click **Change**.
4. On the Manage Service Selection Policies page, modify the information on the General, Service Type, and Service Selection Script pages.

   Important: The IBM Security Identity Manager Server does not verify that the JavaScript is correct. Verify that the JavaScript is correctly coded before using it to define the service selection policy.
5. Click **Submit Now** to save the changes.
6. On the Success page, click **Close**.

Deleting a service selection policy

An administrator can delete a service selection policy, which can be removed when no provisioning policy references it.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Policies** > **Manage Service Selection Policies**.
2. On the Work With Service Selection Policies page, type information about the service selection policy or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Service Selection Policies** table, locate and select a service selection policy, and then click **Delete**.
4. On the Confirm page, review the service selection policy to delete, choose a date and time for the deletion to occur, and then click **Delete**.
5. On the Success page, click **Close**.

Chapter 12. Workflow management

Workflows for entitlements to an account or access can be added, deleted, and modified from the workflow design page. Additionally, you can change workflow properties, escalation, notification, and other workflow activities.

Before you begin

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

Adding an entitlement workflow

As an administrator, you can create a workflow for either an account request or an access request.

Before you begin

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

Before you begin, determine whether additional access control items are needed for the new workflow.

About this task

You can use the Workflow Designer page to add a workflow to either an account request or an access request.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the table that lists the workflows, click **Create**.
3. In the General tab, complete the name and description of the workflow, and select a business unit and service type. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
4. In the **Activities** tab, complete either a simple or an advanced workflow: You can create a simple workflow and convert it to an advanced one if you later decide that you require more advanced capabilities. However, you cannot convert an advanced workflow to a simple one. If you do so, all of your advanced activities are discarded and you start with a new, simple workflow.

Option	Description
Simple	Click to add a workflow that consists of a linear series of approval, mail, or request for information activities. Complete the activity name, participant type, and escalation time and escalation participant type. Then, click **OK**.
Advanced	Click to add an advanced workflow potentially consisting of other types of activities, loops, and conditional branches. The workflow designer applet starts. Using the workflow designer, specify the workflow. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

5. On the Success page, click **Close**.

What to do next

You might associate this workflow with an access or account entitlement.

Changing an entitlement workflow

As an administrator, you can change a workflow for either an account request or an access request.

Before you begin

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

About this task

Before you begin, determine whether changes are also needed to access control items that apply to the workflow.

You can use the Workflow Designer page to change a workflow for either an account request or an access request.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the **Search information** field, type information about the workflow, and click **Search**.

   You can also type information about the service to which the account request workflow is associated, or information about the access to which the access request workflow is associated.

   Note: A search done by **Access** type returns only workflows that have an existing association with the access definition. To see all workflows, select **Workflow** as the search type.

3. In the table that lists the available workflows, select the workflow that you want to modify, and click **Change**.
4. In the General tab or the Activities tab, complete your changes. Then, click **OK**.
5. On the Success page, click **Close**.

What to do next

You might make additional changes to an access control item, or associate this workflow with a different provisioning policy.

Deleting an entitlement workflow

As an administrator, you can delete a workflow for either an account request or an access request.

Before you begin

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

Before you begin, make sure the workflow that you are deleting is no longer referenced by a provisioning policy or access definition.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the **Search information** field, type information about the workflow, and click **Search**.

   You can also type information about the service to which the account request workflow is associated, or information about the access to which the access request workflow is associated.
3. In the table that lists the available workflows, select the workflow that you want to delete, and click **Delete**.
4. In the Confirm page, ensure that you want to proceed, and click then **Delete**.
5. On the Success page, click **Close**.

Creating a mail activity template with the workflow designer

Using the workflow designer, you can create a mail activity template that is based on a default template.

Before you begin

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

About this task

You can use the Workflow Designer page to create a mail activity workflow template that specifies content to be used by mail activities across different workflows.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the table that lists the workflows, click **Create**.
3. In the General tab, complete the name and description of the workflow, and select a business unit and service type. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
4. In the **Activities** tab, click either **Simple** or click **Advanced**.

Option	Description
Simple	1. In the **Simple Activities Definition** table, select an activity for approval, mail, or request for information. Then, click **Go**. 2. Depending on the activity, complete the fields and click **OK**.

Option	Description
Advanced	1. After the workflow designer applet starts, select the Mail node. Then, copy (click and drag) an instance of the Mail node to the Workflow Diagram workspace. Double-click the Mail node instance to open the Properties: Mail Node page. a. In the General tab, make these entries: • In the **Activity ID** field, type a value that identifies the activity, such as `mytesttemplate`. • In the **Recipient** field, select a recipient from the list. • Optionally, type a value for the activity name, and change the default value of the Join Type and Split Type conditions. b. In the Notification tab, either type the tags and other information that you want to be displayed in a customized message notification, by completing the **Subject**, **Text**, and **XHTML** fields as needed. Alternatively, click **Load From Template**. If you load a template, complete these tasks: • In the templates table, select a template. Then, click a button such as **Create Like**. • On the Mail Activity Template page, accept or modify the entries that populate the **Template Name**, **Subject**, **Text**, and **XHTML** fields. • Change the Text and Dynamic entries as needed. Then, click **OK**. c. In the Postscript tab, type any postscript information. d. Click **OK** to complete the task. Depending on the customized steps that you took or the template that you selected, you might need to change the notification recipient.

5. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
6. On the Success page, click **Close**.

Workflow notification properties

Some workflow properties can be configured to apply globally to workflows in IBM Security Identity Manager

IBM Security Identity Manager can be configured with a default escalation period that is used to determine when work items that result from workflow activities are escalated. Activity notification message templates can be customized to send notifications.

All workflow activities are escalated when the escalation period expires. The default escalation period serves as the initial value for newly defined workflow activities. To override the default escalation period, configure the escalation period for a specific activity contained in a workflow.

IBM Security Identity Manager sends email notifications for specific type of account requests and for specific events in the workflow system. The notification can be enabled or disabled based on the request type or event type. The notification template can be customized for each type of notification.

The following is a list of account requests in which an email notification can be generated:

- New account
- New password
- Change account
- Deprovision account
- Suspend account
- Restore account

For access requests that are submitted from the Identity Service Center, an email notification can be generated at the following times:

- Before the access request batch is processed
- After access request batch processing is completed

The following is a list of workflow system events in which an email notification can be generated:

- Activity timeout
- Process timeout
- Process complete
- Approval work item
- Request for input work item
- Work order
- Compliance alert
- Work item reminder

IBM Security Identity Manager can also be configured to send activity notifications and to-do list item reminders through email to workflow participants after a configured amount of time. IBM Security Identity Manager can create default notifications for a type of activity in the form of templates. Notification templates provide a consistent notification style and content across manual activities and system activities such as adding accounts and changing passwords.

Configuring the workflow escalation period

Administrators can set the default escalation limit for work items in workflows.

Before you begin

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

About this task

Before you begin, determine the escalation period that your organization needs for customary escalations.

You can use the Workflow Notification Properties page to change the workflow escalation limit.

Procedure

1. From the navigation tree, select **Configure System** > **Workflow Notification Properties**.
2. On the Workflow Notification Properties page, in the **Escalation Limit** field, specify the time in days, hours, and minutes. Click **OK**.
3. On the Success page, click **Close**.

What to do next

You might also change the default reminder interval and message.

Configuring the work item reminder interval and reminder content

Administrators can set the work item reminder interval and define reminder content.

Before you begin

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

Before you begin, determine the work item reminder interval and the reminder content that your organization needs. Because there are multiple notification templates, you might read the list of templates and their notification content first.

About this task

You can use the Workflow Notification Properties page to change the work item reminder interval and reminder content.

Procedure

1. From the navigation tree, select **Configure System** > **Workflow Notification Properties**.
2. On the Workflow Notification Properties page, you might complete these tasks:
   - In the **Reminder Interval** field, specify the time in days. The value that you enter cannot be less than the time interval for the escalation limit.
   - In the **Reminder Interval** table, select a notification template, and click **Change**. Your changes depend on the content of the template.

3. When your changes are complete, click **OK**.
4. On the Success page, click **Close**.

What to do next

You might also configure notification aggregation (post office).

Enabling workflow notification

You can use the Workflow Notification Properties page to enable workflow notification.

Before you begin

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

Procedure

1. From the navigation tree, select **Configure System** > **Workflow Notification Properties**.
2. On the Workflow Notification Properties page, in the **E-mail Notification Templates** table, locate the template for the notification you want to enable. In the **Status** column of the table, click the popup menu icon, and then click **Enable**.
3. After the value of the field changes to Enabled, click **OK**.
4. On the Success page, click **Close**.

Disabling workflow notification

You can use the Workflow Notification Properties page to disable workflow notification.

Before you begin

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

Procedure

1. From the navigation tree, select **Configure System** > **Workflow Notification Properties**.
2. On the Workflow Notification Properties page, in the **E-mail Notification Templates** table, locate the template for the notification you want to enable. In the **Status** column of the table, click the popup menu icon, and then click **Disable**.
3. After the value of the field changes to Disabled, click **OK**.
4. On the Success page, click **Close**.

Changing a workflow notification template

You can use the Workflow Notification Properties page to change a workflow notification template.

Before you begin

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

Procedure

1. From the navigation tree, select **Configure System** > **Workflow Notification Properties**.
2. On the Workflow Notification Properties page, in the **E-mail Notification Templates** table, select the template for the notification you want to configure. Then, click **Change**.
3. In the Notification Template page, make your changes to the **Template name**, **Subject**, **Plaintext body**, and **XHTML body** fields. Then, click **OK**.
4. On the Workflow Notification Properties page, click **OK**.
5. On the Success page, click **Close**.

Related tasks:

"Manually applying the email notification template changes for canceling a request"
You can use the Workflow Notification Properties page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.3, the email notification template content that includes information about canceling a request is not automatically applied. The template changes that are available with Fix Pack 6.0.0.3 are not automatically applied so that the installation process does not overwrite any custom changes that you might have made to the email templates.

Manually applying the email notification template changes for canceling a request

You can use the Workflow Notification Properties page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.3, the email notification template content that includes information about canceling a request is not automatically applied. The template changes that are available with Fix Pack 6.0.0.3 are not automatically applied so that the installation process does not overwrite any custom changes that you might have made to the email templates.

Before you begin

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

Procedure

1. From the navigation tree, select **Configure System** > **Workflow Notification Properties**.
2. On the Workflow Notification Properties page, in the **E-mail Notification Templates** table, select **Process Completion Template**. Then, click **Change**.
3. In the Notification Template page, modify the **Plaintext body** field by adding this code to the end of the existing code:

```
<JS> if (process.canceledBy != null) { '<RE key="CanceledBy"/>: ' + process.canceledBy; }</JS>
<JS> if (process.canceledBy != null) { '<RE key="DateCanceled"/>: '; }</JS> <RE key="readOnlyDateFormat"><PARM>
<JS> if (process.canceledDate != null) return process.canceledDate.getTime(); else return '';</JS></PARM></RE>
<JS> if (process.canceledBy != null) { '<RE key="CanceledReason"/>:
<JS> (process.canceledJustification == null)? '': process.canceledJustification;</JS>'; }</JS>
```

4. In the Notification Template page, modify the **XHTML body** field by adding this code inside the table:

```
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
   <RE key="CanceledBy"/>:</td><td width="773" class="text-description" bgcolor="white">
   <JS>process.canceledBy;</JS></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
   <RE key="DateCanceled"/>:</td><td width="773" class="text-description" bgcolor="white">
   <RE key="readOnlyDateFormat"><PARM>
   <JS>if (process.canceledDate != null) return process.canceledDate.getTime();
   else return '';</JS>
   </PARM></RE></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
   <RE key="CanceledReason"/>:</td><td width="773" class="text-description" bgcolor="white">
   <JS>process.canceledJustification;</JS></td></tr>
```

   Place the new code inside the table between these two sets of existing code:

```
<pre><JS>Enrole.localize(process.resultDetail, "$LOCALE");</JS></pre></td></tr>
```

   and

```
     </table>
        </td>
                <!-- End Of Notification body -->
```

5. To save the changes, click **OK**.
6. On the Workflow Notification Properties page, click **OK**.
7. On the Success page, click **Close**.

Related tasks:

"Canceling pending requests" on page 461
You can cancel requests that are not completed.

"Changing a workflow notification template" on page 418
You can use the Workflow Notification Properties page to change a workflow notification template.

Sample workflows

This section contains sample workflows.

Sample workflow: manager approval of accounts

In this scenario, an organization has a policy that requires all accounts provisioned on a WinLocal service to be approved by the direct manager of the requestee.

The request for approval is sent to the manager of the requestee, who has two full days to approve the request. The manager might not respond to the request within the allotted time period. Then, the request is escalated to the service owner who has two full days to act on the request. The task is removed from the task list of the manager at this time. If the service owner fails to act on the request within the allotted time, the request fails, and it is canceled by the system.

The manager or service owner might act on the request within the allotted time period. An Approve response sets the process result to Approved and a Reject response sets the process result to Rejected. An Approved result provisions the account and logs the process activity in the audit log. A Rejected result cancels the process and logs the rejection in the audit log.

The graphic demonstrates this business case with the default script nodes RETURN_APPROVED and RETURN_REJECTED, which set the process result based upon participant response. The table identifies the workflow node properties and their values for a workflow named Approval_Example, defined with a service type of WinLocal Profile.

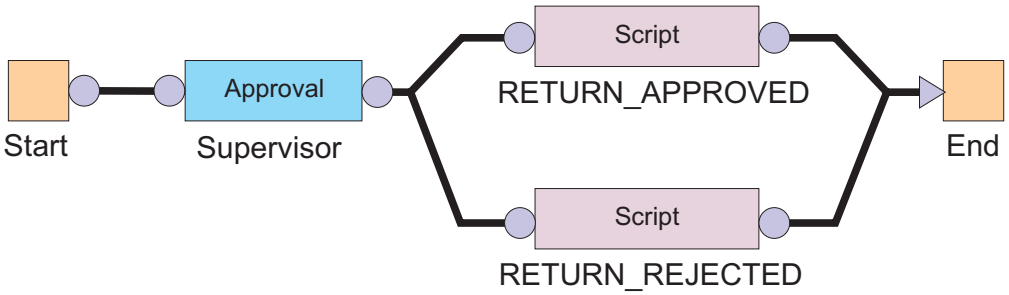


Figure 3. Sample workflow for manager approval

Table 85. Node properties: Sample workflow for manager approval

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Approval	Activity ID	Supervisor
	Participant	Supervisor
	Escalation Participant	Service Owner
	Escalation Limit	2 days
	Join Type	AND
	Split Type	AND
	Entity Type	Account
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] `process.setResult("AA")`
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] `process.setResult("AR")`

Sample workflow: multiple approvals

In this scenario, an organization has a policy in place for provisioning an account on a Windows server that is used for financial applications.

When a request is generated, a service owner must enter the appropriate account information before any approvals can take place. Then the request must be

approved by both the Chief Financial Officer and the direct manager of the requestee. Each approver has one full day to act on the request.

After receiving a result from both approval requests, an email is generated and sent to the direct manager of the requestee. The email details the result and the process completes.

If both participants approve the request, the request is completed and the account is provisioned. If either of the participants rejects the request for approval, the process is completed without provisioning the account and the process result is set to Rejected.

All relevant activity is logged in the Audit Log.

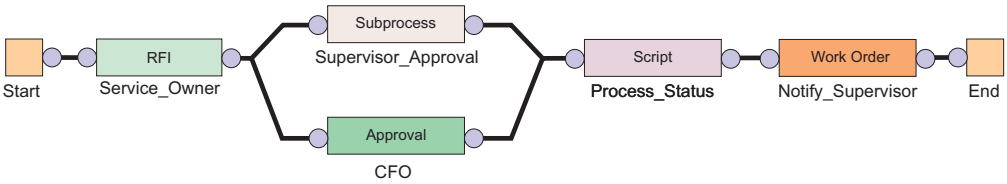


Figure 4. Sample workflow: multiple approvals required

Table 86. Node properties: Sample workflow for multiple approvals

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
RFI	Activity ID	Service_Owner
	Participant	Service_Owner
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
	Entity	WinLocal
Subprocess	Activity ID	Supervisor_Approval
	Subprocess	Workflow created in “Sample workflow: manager approval of accounts”
	Join Type	AND
	Split Type	AND

Table 86. Node properties: Sample workflow for multiple approvals (continued)

Node	Feature	Value
Approval	Activity ID	CFO
	Participant	[Org Role] Chief Financial Officer
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
Script	Activity ID	Process_Status
	Join Type	AND
	Split Type	AND
	JavaScript	`supervisorApproval= process.getActivity("Supervisor_Approval").result Summary cfoApproval=process.getActivity("CFO").resultSummary if(supervisorApproval==activity.APPROVED && cfoApproval==activity.APPROVED) { process.setResult(process.APPROVED) } else { process.setResult(process.REJECTED) }`
Work Order	Activity ID	Notify_Supervisor
	Participant	Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Subject	`New <JS>process.subject;</JS> provisioning request for <JS>process.requesteeName;</JS>`
	Message	Process Result: <JS>process.resultSummary</JS>
End	Activity ID	End
	Join Type	AND
	JavaScript	N/A
Transition Line`Start > Service_Owner RFI`	JavaScript	[Custom] `true`
Transition Line`Service_Owner RFI > Supervisor_Approval Subprocess`	JavaScript	[Custom] `true`
Transition Line`Service_Owner RFI > CFO Approval`	JavaScript	[Custom] `true`
Transition Line`Supervisor_Approval Subprocess > Process_Status Script`	JavaScript	[Custom] `true`
Transition Line`CFO Approval > Process_Status Script`	JavaScript	[Custom] `true`

Table 86. Node properties: Sample workflow for multiple approvals (continued)

Node	Feature	Value
Transition Line Process_Status Script > Notify_Supervisor Work Order		[Custom] true
Transition Line Notify_Supervisor Work Order > End	JavaScript	[Custom] true

Sample workflow: multiple approvals with loop processing

In this scenario, an organization has a policy in place for all new hires. A human resources staff member submits the person information, which initiates a workflow process to provision a Windows account.

A request is sent the immediate manager of the requestee and must first be approved whether the account is okay to be provisioned. If the manager rejects the approval, the account is not provisioned and the process is cancelled. Then the manager is requested to enter the information needed to provision the account. The service owner then reviews the account data to assure the account is created correctly. If any of the account information is incorrect the service owner comments on errors and rejects the request. The request is then sent back to the manager for changes. This process is repeated up to three times or until the Service Owner is satisfied with the account data and approves it. The service owner approval is strictly for approving the RFI data submitted by the manager. The service owner approval has no bearing on the end process result or provisioning of the account.

Even though the service owner is not satisfied with the manager's third correction, the department manager is requested for the approval. After the approval from the department manager, the account is provisioned. If rejected, the account is not provisioned and the process is canceled.

Basically, provisioning a new Windows account requires the approval from both the manager of the requestee and manager of the department. During the process, the account information gets audited from the service owner.

All activities are logged in the audit log.

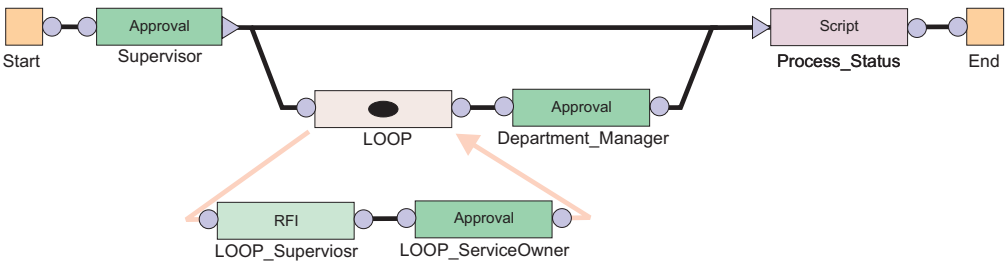


Figure 5. Sample workflow: multiple approvals with loop processing

Table 87. Node properties: Sample workflow for multiple approvals with loop processing

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Approval	Activity ID	Supervisor
	Participant	Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	OR
	Entity Type	Account
Loop	Name	LOOP
	Join Type	AND
	Split Type	AND
	Loop Type	While
	Loop Condition	`(loopcount<=1) || (loopcount <=3 && (process.getActivity ("LOOP_ServiceOwner", loopcount-1)).resultSummary ==activity.REJECTED)`
RFI	Name	LOOP_Supervisor
	Participant	Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
	Entity	WinLocal
Approval	Name	LOOP_ServiceOwner
	Participant	Service Owner
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account

Table 87. Node properties: Sample workflow for multiple approvals with loop processing (continued)

Node	Feature	Value
Approval	Name	Department_Manager
	Participant	[Organizational Role] Department_Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
Script	Activity ID	Process_Status
	Join Type	OR
	Split Type	AND

	JavaScript	[Custom]
		`supervisorApproval=process.getActivity("Supervisor")`
		`.resultSummary`
		`if(supervisorApproval==activity.REJECTED) {`
		`process.setResult(process.REJECTED)`
		`}else if(supervisorApproval==activity.APPROVED) {`
		`departmentManagerApproval=`
		`process.getActivity("Department_Manager")`
		`.resultSummary`
		`if (departmentManagerApproval==activity.APPROVED) {`
		`process.setResult(process.APPROVED)`
		`} else if`
		`(departmentManagerApproval==activity.REJECTED) {`
		`process.setResult(process.REJECTED)`
		`}`
		`}`

End	Activity ID	End
	Join Type	AND
	JavaScript	N/A
Transition Line Start > Supervisor Approval	JavaScript	Custom] `true`
Transition Line Supervisor Approval > LOOP	JavaScript	[Approved] `activity.resultSummary==activity.APPROVED;`
Transition Line Supervisor Approval > Process_Status Script	JavaScript	[Rejected] `activity.resultSummary==activity.REJECTED;`
Loop Begin Transition LineLOOP > LOOP_Supervisor RFI		
Transition LineLOOP_Supervisor RFI > LOOP_ServiceOwner Approval	JavaScript	[Custom] `true`
Loop End Transition LineLOOP_ServiceOwner Approval > LOOP		

Table 87. Node properties: Sample workflow for multiple approvals with loop processing (continued)

Node	Feature	Value
Transition LineLOOP > Department_Manager Approval	JavaScript	[Custom] true
Transition Line Department_Manager Approval > Process_Status Script	JavaScript	[Custom] true
Transition Line Process_Status Script > End	JavaScript	[Custom] true

Sample workflow: RFI and subprocess

This example displays an entitlement workflow that uses an RFI and a subprocess.

For the request to be approved and reach completion, the following actions must occur:

- The workflow initiated by the Subprocess node must be completed with a result of approved.
- The participant defined in the RFI node is sent a request for information.

An approved response must come from the subprocess for the request to continue to the RFI.

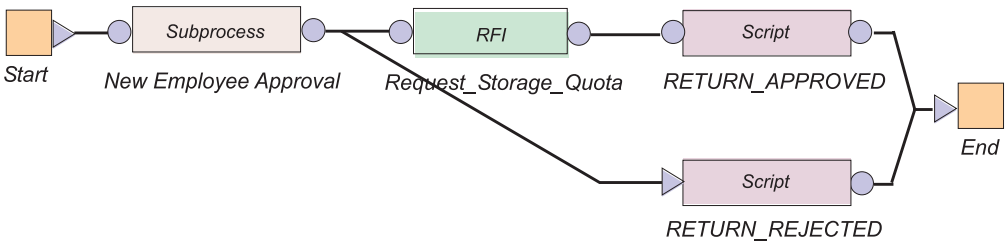


Figure 6. Sample workflow: RFI and subprocess

Table 88. Node properties: Sample workflow with an RFI and a subprocess

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Subprocess	Activity ID	New_Employee_Approval
	Subprocess	Workflow created in "Sample workflow: supervisor approval of accounts"
	Join Type	OR
	Split Type	OR

Table 88. Node properties: Sample workflow with an RFI and a subprocess (continued)

Node	Feature	Value
RFI	Activity ID	Request_Storage_Quota
	Participant	Service Owner
	Escalation Limit	3 days
	Entity Type	Account
	Entity	WinLocalAccount
	Attribute Selection	Max. Storage
	Join Type	OR
	Split Type	OR
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	OR
	Split Type	OR
	JavaScript	`process.setResult (process.APPROVED);`
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	OR
	Split Type	OR
	JavaScript	`process.setResult (process.REJECTED);`
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A
Transition Line`Start > New Employee Approval`	JavaScript	[Custom] `true`
Transition Line`New Employee Approval > Request Storage Quota`	JavaScript	[Approved] `activity.resultSummary ==activity.APPROVED;`
Transition Line`New Employee Approval > RETURN_REJECTED`	JavaScript	[Rejected] `activity.resultSummary ==activity.REJECTED;`
Transition Line`Request Storage Quota > RETURN_APPROVED`		[Custom] `true`
Transition Line`RETURN_APPROVED > End`	JavaScript	[Custom] `true`
Transition Line`RETURN_REJECTED > End`	JavaScript	[Custom] `true`

Sample workflow: approval loop

This example displays a workflow that loops an Approval node.

In this workflow, the manager approval is set within the Loop node. The manager approval repeats five times before failing if an approved or rejected response is not received within the escalation Limit.

Conditions for the transition lines to the RETURN_APPROVED and RETURN_REJECTED script nodes must be defined to retrieve and evaluate the results of the Approval node. The loop node does not return a response from the Approval.

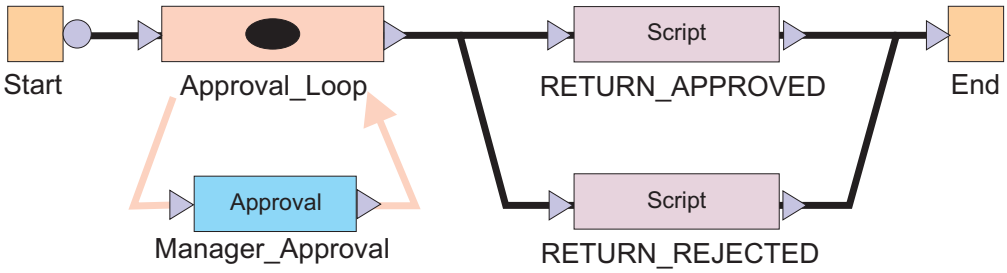


Figure 7. Sample workflow: approval loop

Table 89. Node properties: Sample workflow with an approval loop

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Loop	Activity ID	Approval_Loop
	Loop Type	Until
	Loop Condition	`var flag = approvalFlag.get();return (loopcount <= 5 && (flag != "APPROVED" && flag != "REJECTED"));`
	Split Type	OR
	Join Type	OR
Approval	Activity ID	Manager_Approval
	Participant	Manager
	Escalation Limit	1 day
	Entity Type	Account
	Postscript	`if (activity.resultSummary == activity.APPROVED) { approvalFlag.set("APPROVED");} else if (activity.resultSummary == activity.REJECTED){approvalFlag.set("REJECTED");}`
	Join Type	OR
	Split Type	OR
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	OR
	Split Type	OR
	JavaScript	`process.setResult(process.APPROVED);`
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	OR
	Split Type	OR
	JavaScript	`process.setResult(process.REJECTED);`

Table 89. Node properties: Sample workflow with an approval loop (continued)

Node	Feature	Value
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A
Transition Line Start > Approval Loop	JavaScript	[Custom] true
Transition Line Approval Loop > RETURN_APPROVED	JavaScript	[Custom] approvalFlag.get() == "APPROVED"
Transition Line Approval Loop > RETURN_REJECTED	JavaScript	[Custom] approvalFlag.get() == "REJECTED"
Transition LineRETURN_APPROVED > END	JavaScript	[Custom] true
Transition LineRETURN_REJECTED > END	JavaScript	[Custom] true
Relevant DataapprovalFlag	ID	approvalFlag
	Description	Data for storing the last approval result
	Context	N/A
	Type	String
	Default Value	FALSE

Sample workflow: mail activity

Use the Workflow Designer page to create a mail activity workflow template that specifies content to be used by mail activities across different workflows.

Use this page to specify the contents and recipient of an email message. You can also create, change, or delete email templates used for defining contents of mail activities. To create a notification that uses an existing notification template as its initial content, or to create an entirely new notification, complete these steps:

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that appears, in the table that lists the workflows, click **Create**.
3. In the **General** tab, complete the name and description of the workflow, and select a business unit and service type.
4. In the **Activities** tab, click **Simple**.
5. In the **Simple Activities Definition** table, select **Create a mail activity**. Then, click **GO**.
6. In the Mail Activity page, complete the following fields:

   Activity name
   Provides a name for the mail activity.

   Recipient type
   Select a recipient for mail from the list. You might select **User name** or **Group**. An additional field is displayed for you to search for and specify a specific user or group that is not in the list.

   Load from Template
   Click to select the mail template from which to load the content and to

do other mail template management tasks. After loading the contents from a mail template, editing the content in the mail activity will affect only the mail activity, not the template.

Subject
Provides a description of the activity to the recipient of the mail notification.

Plaintext body
Provides additional details to the recipient that describe the outcome of the activity, in plaintext format. For example, an account or access request was approved.

XHTML body
Provides additional details to the recipient that describe the outcome of the activity, in XHTML format. For example, an account or access request was denied.

7. When the fields are complete, click **OK**.
8. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
9. On the Success page, click **Close**.

Sample workflow: sequential approval for user recertification with packaged approval node

This scenario shows an organization policy that requires user recertification to be approved by two levels of approvers. The first approver submits decisions that are reviewed by the second approver. The second approver can change the decisions made by the first approver and then submit the final decisions. The request in this scenario is for recertification approval of user resources (accounts, groups, or roles).

For the request to be approved and reach completion, the following actions must occur:

1. A user sends the request to an IBM Security Identity Manager user (*Approver1*).
2. *Approver1* has one day to approve the request.
3. *Approver1* submits decisions for the item in the To-Do list.
4. *Approver1* sends the request to the second Security Identity Manager user (*Approver2*).
5. *Approver2* can view the decisions from *Approver1* in the To-Do list.
6. *Approver2* can make and submit additional decisions.
7. Security Identity Manager does the recertification of the user resources based on decisions of *Approver2*.

The following workflow graphic demonstrates this business case. The workflow uses the two packaged approval nodes *DECISION_OF_APPROVER1* and *DECISION_OF_APPROVER2* in a sequence. The decisions from *Approver1* are stored in the `ApprovalDocument` so that *Approver2* can view them before submitting final decisions.

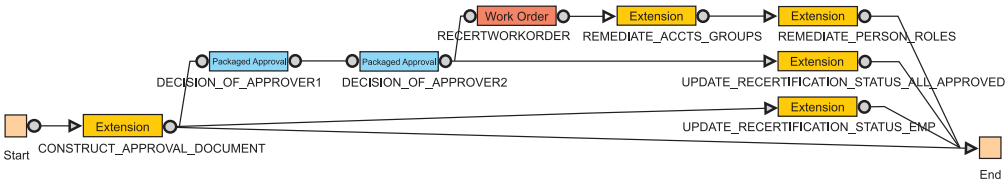


Figure 8. Sample workflow: sequential approval with packaged approval node

Table 90 identifies the workflow node properties and values for *User_Recertification_Sequential_Approval_Example*.

Table 90. Node properties: sample workflow for packaged approvals

Node	Feature	Value
Start	Activity ID	START
	Activity Name	Start Activity
	Join Type	AND
	Split Type	AND
	JavaScript	`RejectionAction.set('SUSPEND')`
Extension	Activity ID	CONSTRUCT_APPROVAL_DOCUMENT
	Activity Name	CONSTRUCT_APPROVAL_DOCUMENT
	Description	Get all account and access recertification targets for person extension for recertification.
	Join Type	OR
	Split Type	AND
	Extension Name	constructApprovalDocument(Person person, RecertificationPolicy policy)
Packaged Approval	Activity ID	DECISION_OF_APPROVER1
	Participant	Approver1
	Escalation Limit	1 day
	Skip Escalation	Checked
	Join Type	AND
	Split Type	AND

	Postscript	`if (activity.resultSummary == activity.TIMEOUT) {`
		`  var auditMessage = "Recertification period exceeded with no action taken, all items were approved based on policy configuration.";`
		`  activity.setResult(activity.TIMEOUT, auditMessage);`
		
		`  var doc = ApprovalDocument.get();`
		`  doc.setDecisionCodeForAllItems(activity.APPROVED);`
		`  ApprovalDocument.set(doc);`
		
		`  RecertificationWorkflow.auditTimeout(Entity.get(), Policy.get(), doc, false, true);`
		`} else if (activity.resultSummary != activity.FAILED) {`
		`  RecertificationWorkflow.auditCompletion(Entity.get(), Policy.get(), ApprovalDocument.get(), false, true);`
		`}`

Packaged Approval	Activity ID	DECISION_OF_APPROVER2
	Activity Name	$ITIM_RECERTIFY
	Participant	Approver2
	Escalation Limit	10 days
	Skip Escalation	Checked
	Join Type	AND
	Split Type	AND

	Postscript	`if (activity.resultSummary == activity.TIMEOUT) {`
		`  var auditMessage = "Recertification period exceeded with no action taken, all items were approved based on policy configuration.";`
		`  activity.setResult(activity.TIMEOUT, auditMessage);`
		
		`  var doc = ApprovalDocument.get();`
		`  doc.setDecisionCodeForAllItems(activity.APPROVED);`
		`  ApprovalDocument.set(doc);`
		
		`  RecertificationWorkflow.auditTimeout(Entity.get(), Policy.get(), doc);`
		`} else if (activity.resultSummary != activity.FAILED) {`
		`  RecertificationWorkflow.auditCompletion(Entity.get(), Policy.get(), ApprovalDocument.get());`
		`}`

Mail	Activity ID	RECERTMAIL
	Activity Name	$RECERTMAIL
	Recipient	Requestee
	Join Type	AND
	Split Type	AND
Extension	Activity ID	REMEDIATE_ACCTS_GROUPS
	Activity Name	REMEDIATE_ACCTS_GROUPS
	Description	Performs account, group, and access remediation
	Join Type	OR
	Split Type	AND
	Extension Name	remediateAccountsAndGroups(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)

Table 90. Node properties: sample workflow for packaged approvals (continued)

Node	Feature	Value
Extension	Activity ID	REMEDIATE_PERSON_ROLES
	Activity Name	REMEDIATE_PERSON_ROLES
	Description	Performs role remediation, including policy enforcement for the person
	Join Type	OR
	Split Type	AND
	Extension Name	remediateRoleMemberships(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Activity Name	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Description	Updates recertification status
	Join Type	OR
	Split Type	AND
	Extension Name	updateRecertificationStatusAllApproved(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Activity Name	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Description	Updates recertification status
	Join Type	OR
	Split Type	AND
	Extension Name	updateRecertificationStatusEmptyDocument(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)
End	Activity ID	END
	Activity Name	End Activity
	Join Type	OR
	Split Type	AND

Table 91 identifies the link properties and their values for the packaged approval sample workflow.

Table 91. Link properties: sample workflow for packaged approvals

From	To	Feature	Value
Start	Extension	Name	startToConstructApprovalDocumentExtension
		Description	Start node to construct approval document extension
START	CONSTRUCT_APPROVAL_DOCUMENT	Custom Condition	true
Extension	Packaged Approval	Name	constructApprovalDocumentExtensionToApprover1Approval
		Description	Construct approval document extension to Approver1 approval node
CONSTRUCT_APPROVAL_DOCUMENT	DECISION_OF_APPROVER1	Custom Condition	activity.resultSummary == activity.SUCCESS
Extension	Extension	Name	contructApprovalDocumentExtensionToUpdateStatusEmpty
		Description	Construct approval document extension to update status for empty document
CONSTRUCT_APPROVAL_DOCUMENT	UPDATE_RECERTIFICATION_STATUS_EMPTY	Custom Condition	activity.resultSummary == activity.WARNING
Extension	End	Name	constructApprovalDocumentExtensionToEnd
		Description	Construct approval document extension to end node
CONSTRUCT_APPROVAL_DOCUMENT	END	Custom Condition	activity.resultSummary != activity.SUCCESS && activity.resultSummary != activity.WARNING
Packaged Approval	Packaged Approval	Name	approver1ApprovalToApprover2Approval
		Description	Approver1 approval node to Approver2 approval node
DECISION_OF_APPROVER1	DECISION_OF_APPROVER2	Custom Condition	activity.resultSummary != activity.FAILED
Packaged Approval	Mail	Name	approver2ApprovalToMail
		Description	Approver2 approval node to mail node
DECISION_OF_APPROVER2	RECERTMAIL	Custom Condition	(activity.resultSummary != activity.FAILED) && (Approvalocument.get().containsDecisionCode(activity.REJECTED))
Packaged Approval	Extension	Name	approver2ApprovalToUpdateStatus
		Description	Approver2 approval node to update recertification status
DECISION_OF_APPROVER2	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	Custom Condition	(activity.resultSummary != activity.FAILED) && (!ApprovalDocument.get().containsDecisionCode(activity.REJECTED))
Mail	Extension	Name	mailToRemediateAccts
		Description	Mail node to remediate accounts, groups, and accesses
RECERTMAIL	REMEDIATE_ACCTS_GROUPS	Custom Condition	true
Extension	Extension	Name	remediateAcctsToRemediateRoles
		Description	Remediate accounts, groups, and accesses to remediate roles
REMEDIATE_ACCTS_GROUPS	REMEDIATE_PERSON_ROLES	Custom Condition	true
Extension	End	Name	remediateRolesToEnd
		Description	Remediate roles to end node
REMEDIATE_PERSON_ROLES	END	Custom Condition	true

Table 91. Link properties: sample workflow for packaged approvals (continued)

From	To	Feature	Value
Extension UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	End END	Name	updateStatusToEnd
		Description	Update recertification status to end node
		Custom Condition	true
Extension UPDATE_RECERTIFICATION_STATUS_EMPTY	End END	Name	updateStatusEmptyToEnd
		Description	Update status for empty document to end node
		Custom Condition	true

Sample workflow: packaged approval combined with simple approval node

This scenario shows an organization with a policy that requires user recertification. User recertification validates user resources (accounts, groups, or roles).

IBM Security Identity Manager does the request based on the following decisions:

- The request for recertification approval of user roles is sent to the respective role owners.
- The request for recertification approval of user accounts and groups is sent to the manager of the user to be recertified.

The following workflow graphic demonstrates this business case:

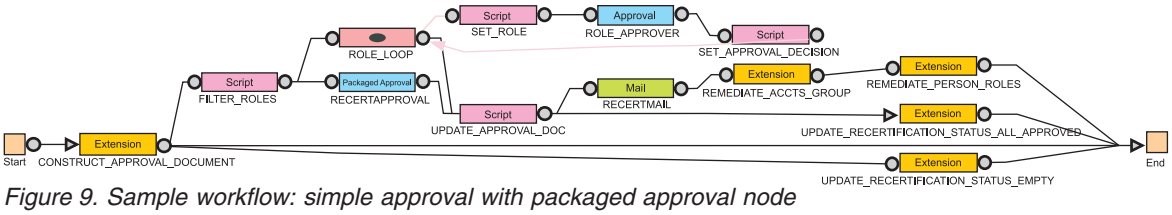


Figure 9. Sample workflow: simple approval with packaged approval node

Table 92 identifies the workflow node properties and values for *User_Recertification_Simple_Approval_Example*.

Table 92. Sample workflow node properties: Simple approval for user recertification with packaged approval node

Node	Feature	Value
Start	Activity ID	Start
	Activity Name	Start Activity
	Join Type	AND
	Split Type	AND
	JavaScript	RejectionAction.set('SUSPEND');
Extension	Activity ID	CONSTRUCT_APPROVAL_DOCUMENT
	Activity Name	CONSTRUCT_APPROVAL_DOCUMENT
	Description	Get all account and access recertification targets for person extension for recertification
	Join Type	OR
	Split Type	AND
	Extension Name	constructApprovalDocument(Person person, RecertificationPolicy policy)

Table 92. Sample workflow node properties: Simple approval for user recertification with packaged approval node (continued)

Node	Feature	Value
Script	Activity ID	FILTER_ROLES
	Activity Name	FILTER_ROLES
	Description	Extracts roles from the approval document and creates a temporary approval document with the roles
	Join Type	AND
	Split Type	AND

	JavaScript	`var updatedDoc=ApprovalDocument.get();`
		`var tempDoc=new PackagedApprovalDocument();`
		`TemporaryDocument.set(tempDoc);`
		`var tempRoles=new Array();`
		`var roleItems=updatedDoc.getItemsByType`
		`(ApprovalDocument.get().TYPE_ROLE);`
		`for(var i=0;i<roleItems.length;i++)`
		`{`
		`updatedDoc.removeItem(roleItems[i]);`
		`var roledn= roleItems[i].getValue().dn;`
		`var role=new Role(roledn);`
		`tempRoles.push(role);`
		`RolesThere.set("true");`
		`}`
		`Roles.set(tempRoles);`
		`ApprovalDocument.set(updatedDoc);`
		`var accountsCount=updatedDoc.getItemsByType`
		`(ApprovalDocument.get().TYPE_ACCOUNT);`
		`var groupCount=updatedDoc.getItemsByType`
		`(ApprovalDocument.get().TYPE_GROUP);`
		`if((!accountsCount.length==0||!groupCount.length==0))`
		`{`
		`OnlyRoles.set("false");`
		`}`
		`else`
		`{`
		`OnlyRoles.set("true");`
		`}`

Packaged Approval	Activity ID	RECERTAPPROVAL
	Activity Name	ITIM_RECERTIFY
	Participant	Manager
	Escalation Participant	Participant Type
	Escalation Limit	10 days
	Skip Escalation	Checked
	No Timeout Action	Unchecked
	Join Type	AND
	Split Type	AND
Loop	Activity ID	ROLE_LOOP
	Activity Name	ROLE_LOOP
	Description	This loop is required to iterate through the roles.
	Join Type	AND
	Split Type	AND
	Loop Type	Until
	Loop Condition	`return loopcount<=Roles.get().length;`
Script	Activity ID	UPDATE_APPROVAL_DOC
	Activity Name	UPDATE_APPROVAL_DOC
	Description	Gets the role information from the temporary approval document and updates in into the approval document
	Join Type	AND
	Split Type	AND

	JavaScript	`var approvalDoc=ApprovalDocument.get();`
		`var tempDoc=TemporaryDocument.get();`
		`var roleItems=tempDoc.getItemsByType`
		`(TemporaryDocument.get().TYPE_ROLE);`
		`for(var i=0;i<roleItems.length;i++)`
		`{`
		`approvalDoc.addItem(roleItems[i]);`
		`}`
		`ApprovalDocument.set(approvalDoc);`

Script	Activity ID	SET_ROLE
	Activity Name	SET_ROLE
	Description	Sets the role in relevant data
	Join Type	AND
	Split Type	AND

	JavaScript	`var roles=Roles.get();`
		`var role=roles[loopcount-1];`
		`RoleHolder.set(role);`

Work Order	Activity ID	RECERTWORKORDER
	Activity Name	RECERTWORKORDER
	Escalation Limit	9 days
	Join Type	AND
	Split Type	AND

Table 92. Sample workflow node properties: Simple approval for user recertification with packaged approval node (continued)

Node	Feature	Value
Approval	Activity ID	ROLE_APPROVER
	Activity Name	ROLE_APPROVER
	Participant	Custom: var owner=RoleHolder.get().getProperty("owner")[0]; return new Participant(ParticipantType.USER,owner);
	Escalation Participant	Participant Type
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Organizational Role
Mail	Activity ID	RECERTMAIL
	Activity Name	RECERTMAIL
	Recipient	Person (With Email Account)
	Join Type	AND
	Split Type	AND
Extension	Activity ID	REMEDIATE_ACCTS_GROUPS
	Activity Name	REMEDIATE_ACCTS_GROUPS
	Description	Does account, group, and access remediation
	Join Type	AND
	Split Type	AND
	Extension Name	remediateAccountsAndGroups(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)
Script	Activity ID	SET_APPROVAL_DECISION
	Activity Name	SET_APPROVAL_DECISION
	Description	Updates the temporary approval document with the role and its decision
	Join Type	AND
	Split Type	AND

	JavaScript	`var updatedDoc=TemporaryDocument.get();`
		`var res=result.get();`
		`var roleItems=Roles.get();`
		`var roleItem=new PackagedApprovalItem`
		`(ApprovalDocument.get().TYPE_ROLE,roleItems[loopcount-1],res);`
		`var dec=roleItem.getDecisionCode()`
		`updatedDoc.addItem(roleItem);`
		`TemporaryDocument.set(updatedDoc);`

Extension	Activity ID	REMEDIATE_PERSON_ROLES
	Activity Name	REMEDIATE_PERSON_ROLES
	Description	Does role remediation, including policy enforcement for the person
	Join Type	AND
	Split Type	AND
	Extension Name	remediateRoleMemberships(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Activity Name	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Description	Updates recertification status with all approved user resources
	Join Type	OR
	Split Type	AND
	Extension Name	updateRecertificationStatusAllApproved(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Activity Name	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Description	Updates recertification status with no user resources
	Join Type	AND
	Split Type	AND
	Extension Name	updateRecertificationStatusEmptyDocument(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)
End	Activity ID	End
	Activity Name	End Activity
	Join Type	OR
	Split Type	AND
	JavaScript	

Table 93 identifies the link properties and values for the simple approval node.

Table 93. Link properties: Simple approval for user recertification

From	To	Feature	Value
Start	Extension `CONSTRUCT_APPROVAL_DOCUMENT`	Name	startToConstructApprovalDocumentExtension
		Description	Start node to construct approval document extension
		Custom Condition	`true`
Extension `CONSTRUCT_APPROVAL_DOCUMENT`	Script `FILTER_ROLES`	Name	ConstructApprovalDocumentExtensionToFilterRolesScript
		Description	Construct approval document extension to filter roles script
		Custom Condition	`activity.resultSummary == activity.SUCCESS`

Table 93. Link properties: Simple approval for user recertification (continued)

From	To	Feature	Value
Extension CONSTRUCT_APPROVAL_DOCUMENT	End	Name	ConstructApprovalDocumentExtensionToEnd
		Description	Construct approval document extension to end node
		Custom Condition	activity.resultSummary != activity.SUCCESS && activity.resultSummary != activity.WARNING
Extension CONSTRUCT_APPROVAL_DOCUMENT	Extension UPDATE_RECERTIFICATION_STATUS_EMPTY	Name	ConstructApprovalDocumentExtensionToUpdateStatusEmpty
		Description	Construct approval document extension to update status for empty document
		Custom Condition	activity.resultSummary == activity.WARNING
Script FILTER_ROLES	Packaged Approval RECERTAPPROVAL	Name	FilterRolesScriptToRecertApproval
		Description	Filter roles script to recert approval
		Custom Condition	OnlyRoles.get()=="false"
Script FILTER_ROLES	Loop ROLE_LOOP	Name	FilterRolesScriptToRoleLoop
		Description	Filter roles script to role loop
		Custom Condition	RolesThere.get()=="true"
Loop ROLE_LOOP	Script COMBINE_APPROVAL_DOC	Name	RoleLoopToCombineApprovalDocScript
		Description	Role loop to combine approval document script
		Custom Condition	true
Script COMBINE_APPROVAL_DOC	Packaged Approval RECERTAPPROVAL	Name	CombineApprovalDocScriptToRecertApproval
		Description	Combine approval document script to recert approval
		Custom Condition	true
Script COMBINE_APPROVAL_DOC	Mail RECERTMAIL	Name	CombineApprovalDocScriptToMail
		Description	Combine approval document script to mail node
		Custom Condition	(activity.resultSummary != activity.FAILED) && (ApprovalDocument.get().containsDecisionCode(activity.REJECTED))
Script COMBINE_APPROVAL_DOC	Extension UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	Name	CombineApprovalDocScriptTo
		Description	Combine approval document script to
		Custom Condition	(activity.resultSummary != activity.FAILED) && (!ApprovalDocument.get().containsDecisionCode(activity.REJECTED))
Script SET_ROLE	Approval ROLE_APPROVER	Name	SetRoleScriptToRoleApproverApproval
		Description	Set role script to role approver approval
		Custom Condition	true
Approval ROLE_APPROVER	Script SET_APPROVAL_DECISION	Name	RoleApproverApprovalToSetApprovalDecisionScript
		Description	Role approver approval to set approval decision script
		Custom Condition	true
Mail RECERTMAIL	Extension REMEDIATE_ACCTS_GROUPS	Name	mailToRemediateAccts
		Description	Mail node to remediate accounts, groups, and accesses
		Custom Condition	true
Extension REMEDIATE_ACCTS_GROUPS	Extension REMEDIATE_PERSON_ROLES	Name	remediateAcctsToRemediateRoles
		Description	Remediate accounts, groups, and accesses to remediate roles
		Custom Condition	true
Extension REMEDIATE_PERSON_ROLES	End	Name	remediateRolesToEnd
		Description	Remediate roles to end node
		Custom Condition	true
Extension UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	End	Name	updateStatusToEnd
		Description	Update recertification status to end node
		Custom Condition	true
Extension UPDATE_RECERTIFICATION_STATUS_EMPTY	End	Name	updateStatusEmptyToEnd
		Description	Update status for empty document to end node
		Custom Condition	true

Table 94 identifies the relevant data used in the simple approval node.

Table 94. Relevant Data

ID	Type
ApprovalDocument	PackagedApprovalDocument
Roles	List
RoleHolder	OrgRole
TemporaryDocument	PackagedApprovalDocument
RejectionAction	String
result	String
OnlyRoles	String
RolesThere	String

Sample workflow: access owner approval

In this scenario, an organization has a policy that requires access to be provisioned for a user to access an application.

Note that this example applies only to group accesses. It does not apply to roles that are exposed as accesses. See `${ISIM_HOME}/extensions/6.0/examples/workflow/roleApproval/index.html` for examples of configuration changes needed to require or skip access owner (or other) approval for role-based examples.

The access request must be approved by the access owner. The request for approval is sent to the access owner, who has two full days to approve the request. The access owner might not respond within the allotted period. In that case, the request is removed from the task list of the access owner and is escalated to the service owner. The service owner then has two full days to act on the request. If the service owner fails to act on the request within the allotted time, the request fails, and is canceled by the system.

The access owner or the service owner might act on the request within the allotted time period. An Approve response sets the process result to Approved and a Reject response sets the process result to Rejected. An Approved result provisions the access and logs the process activity in the audit log. A Rejected result cancels the process and logs the rejection in the audit log.

The graphic demonstrates this business case with the default script nodes RETURN_APPROVED and RETURN_REJECTED, which set the process result based upon participant response. The table identifies the workflow node properties and their values for the workflow.

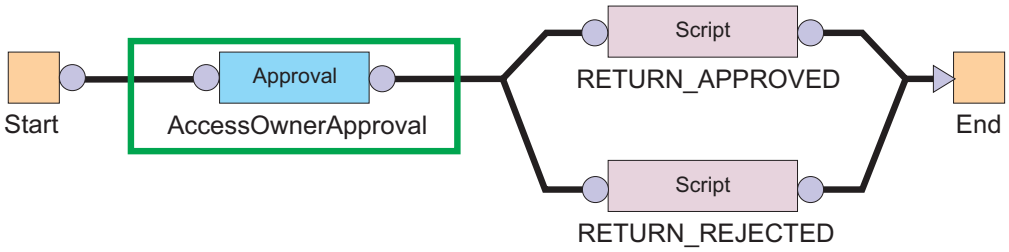


Figure 10. Sample workflow for access request

Table 95. Node properties: Sample workflow for access request

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Approval	Activity ID	AccessOwnerApproval
	Participant	Access Owner
	Escalation Participant	Service Owner
	Escalation Limit	2 days
	Join Type	AND
	Split Type	AND
	Entity Type	UserAccess

Table 95. Node properties: Sample workflow for access request (continued)

Node	Feature	Value
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] `process.setResult("AA")`
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] `process.setResult("AR")`

Chapter 13. Activity administration

You can manage your activities to view your activities, approve and reject requests, and complete work order activities. You can provide information for a request to proceed, approve and reject recertification requests, complete compliance alerts, and delegate activities to other users.

Use the View Activities page to lock, unlock, forward, and respond to action items.

Use the View Activities by User page to view and complete items for other users.

Use the Delegate Activities page to delegate activities to another user when you are not available to manage them.

System administrators can view and respond to all user activity lists. However, system administrators cannot lock work items unless they meet the criteria of being a potential owner of the item.

Activities

An activity is an action item that occurs in your to-do list as part of a workflow process and requires your action. The types of activities are approval requests, work order requests, requests for information, compliance alerts, and recertifications.

Activities are created by requests from other users that require additional information, approval of a request, or for completion of a task. Requests for these users occur as activities for the person who does the action. These activities must be completed for the request to be completed. In some cases, requests are sent to multiple participants who are authorized to complete them.

If you do not complete an activity in the allotted amount of time, it might escalate to another user.

You can also delegate all of your activities for a specified period, if you are unavailable for that time.

Approval activities

An approval activity occurs in the activities list of the user who is prompted to approve or reject a request. Approval activities in your activities list are part of workflow processes that require your response before they can be completed.

If the request is approved, the next activity in the workflow is processed. If, however, the request is rejected, the workflow stops and no additional activities are processed.

If you submit a request that must be approved, the approval activity is sent to all participants in the assigned group except to the user who makes the request. You might be a member of the group who normally approves requests. If you are the person who makes the request, you do not see the approval activity in your activities list.

If a timeout occurs, the Activity Result Summary Code is set to SF (failed). If a participant resolution failure occurs, the Activity Result Summary Code can take the following values:

AA (approved)
If the request is submitted by the system administrator, the request is automatically approved by the system administrator. The approval occurs even though the system administrator is not explicitly set as an escalation participant. The result is set to Approved.

SF (failed)
The Approval activity ends with result set to Failed, if:

- The request is submitted by a non-admin user.
- The escalation participant is not defined at all.

  Note: This result is true even when the requester is the system administrator.
- The participant resolution failed.

If the property enrole.workflow.skipapprovalforrequester is set to true in enRole.properties file and the requester is identified as one of the participant users, the approval is completely skipped. The Activity Result Summary Code is set to AA (approved). When an RFI activity times out or fails because of participant resolution failure, the Activity Result Summary Code is set to SF (failed) for both cases.

Approval states

When you view the status of an approval, the approval activity is in one of several states.

The states of an approval activity can be viewed only by the user who submitted the request. Table 96 describes each approval activity state.

Table 96. Descriptions of the states of approval activities

Approval activity state	Description
Approved	The account request was approved, and the next activity in the workflow is processed.
Rejected	The account request was rejected. No additional activities are processed.
Pending	No action was taken to complete the approval.

Request for information activities

A request for information is displayed in the activities list of the user who must process a request. It prompts the user to supply information about the request.

Request-for-information activities in your activities list are part of workflow processes that require your response before they can be completed. For example, a user submits an account request but does not have the knowledge required to specify a value for a particular attribute. The system administrator creates a process to send the request to a more knowledgeable user. That user can then specify the appropriate value for the attribute.

Request for information (RFI) states

When you view the status of a request, the request for information (RFI) activities might be in one of several states.

The states of an RFI activity can be viewed only by the user who submitted the request. The following table shows a description of each RFI state.

Table 97. Descriptions of the states of RFIs

Request state	Description
Canceled	A pending request is canceled and any action items associated with the request are canceled.
Escalated	Because the original approver did not complete the RFI in the allotted amount of time, the RFI was sent to another approver.
Failed	The activity could not be completed. No further activity occurs.
Participant Resolution Failed	The activity could not be completed because the approver was deleted from the system.
Pending	No action was taken to complete the activity.
Submitted	The activity was submitted for approval.
Success	The RFI was successfully completed.
Terminated	The process run fails with an unknown exception.
Timeout	The specified amount of time to complete an activity passed. The activity is completed and a new activity is created and sent to the escalation participant.
Warning	The activity was partially completed. A problem occurred, preventing the work order from being successfully completed.

Related reference:

ACTIVITY table

Work order activities

A work order activity is displayed in the to-do list of the user who is prompted to do an activity and respond that it is completed. Work order activities in your to-do list are part of workflow processes that require your response before they can be completed.

Work order activities are displayed in your to-do list and consist of action items that you must complete outside the system. For example, you can be assigned a work order to have an office key made for a new employee. After you complete the work order activity, you enter the outcome of the work order when you complete the activity in IBM Security Identity Manager.

Work order states

When you view the status of a work order, the work order activity is in one of several states.

The states of a work order activity can be viewed only by the user who submitted the request. Table 98 on page 444 gives a description of each work order state.

Table 98. Descriptions of the states of work order requests

Work order state	Description
Success	The work order was successfully completed, and the next activity in the workflow is processed.
Warning	The work order was partially completed. A problem occurred, preventing the work order from being successfully completed. No additional activities are processed.
Failure	The work order was not completed. No additional activities are processed.
Pending	No action was taken to complete the work order.

Compliance alert activities

A compliance alert creates an activity for the user who is not in compliance. The user or an administrator can respond.

Compliance rules can govern access to an account and that are required in a resource or asset.

The compliance alert activity is added to the activity list for the user who is not in compliance. The user typically must update the account or attribute that is not in compliance.

An administrator may also perform the following actions:

- remove a noncompliant account
- update noncompliant attributes in a resource or asset
- change the due date of compliance alert activities for any user

See also the following topics:

- "Configuring compliance alert rules" on page 164
- "Completing a compliance alert activity" on page 449
- "Deferring policy compliance alerts" on page 450

Recertification activities

A recertification activity is displayed in the list of the user who is prompted to perform an activity and respond that it is complete. Recertification activities are part of workflow processes that require your response before they can be complete.

Recertification activities are displayed in your activities list. Three types of recertification activities exist:

Access
Certifies whether an access is still required.

Account
Certifies whether an account is still required.

User Certifies whether the roles, accounts, and accesses for a specific user are still required.

To-do lists

A to-do list is a list of activities that assigned to you that you must complete before a request can be completed. The to-do list is where you view and complete action items that assigned to you.

A to-do list is a collection of outstanding activities. Activities are often grouped such that you can view and complete them as a single unit, improving your productivity.

Action items in an administrator's to-do list are part of workflow processes that require the administrator's participation before they can complete.

You might submit a request that must be approved. The approval activity is sent to all participants in the assigned group except to the user who makes the request. You might be member of the group who normally approves requests. If you are the person who makes the request, you do not see the approval activity in your to-do list.

Requests

Requests are items that initiate a workflow, or work order for manual service operations, and instigate the various activities of a workflow.

There are many different types of requests that can occur, such as requesting changes to accounts, adding and modifying users, and changing policies. Some requests might require the completion of a to-do activity by another user, such as an approval or recertification. Other requests might complete without any action required.

Note: Requests that do not initiate a workflow, such as Orphan Account Requests do not get displayed in the pending or completed requests.

Requests can involve several steps to complete. Each step might require different users to complete an action. You can view the status of a request by viewing pending requests or all requests that are both pending and completed.

Completed requests are requests that completed processing. The completion of a request does not mean that it was successful. Requests might fail, might complete with a warning message, or might be canceled while in a pending state.

Pending requests are requests that are submitted but are not finished. These requests might be in the process of running or might require the completion of a workflow activity, such as a recertification or approval activity.

Escalation

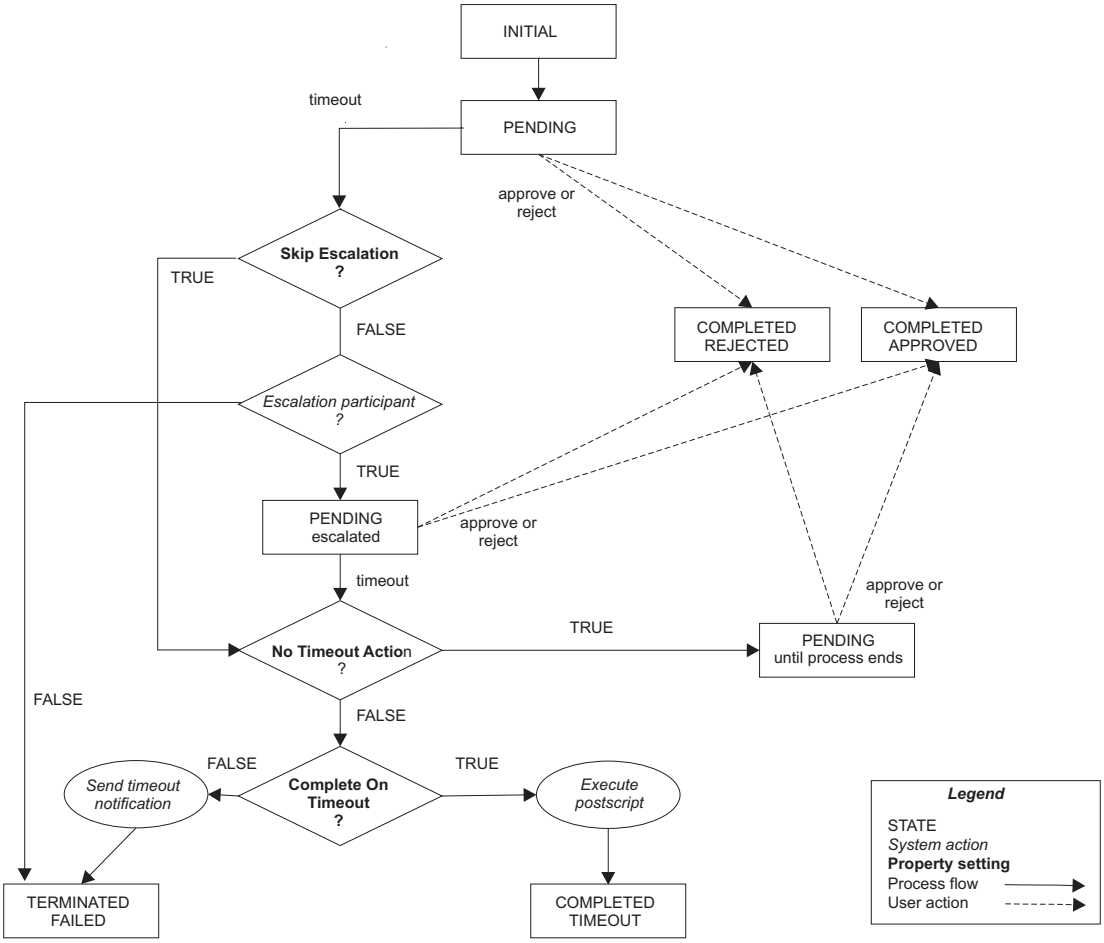
The escalation period specifies the period within which an assigned party must do an activity before it is designated to a specified escalation participant.

Escalation is the period in which the participant must process approvals, requests for information, work orders, compliance alerts, and recertifications. If the participant does not complete the activity by the escalation date, the activity is sent to the escalation participant and the escalation period restarts. Activity is terminated if none of the participants act on it. Activity is sent to the system administrator only if participant resolution fails.

Escalation behavior is controlled through properties on approval, RFI, or work order nodes. The following properties affect escalation behavior:

- **Skip Escalation**
- **No Timeout Action**
- **Complete on Timeout**

The following figure shows a flow diagram that illustrates how each property affects the process.



The following list describes escalation process that is pictured in the diagram.

1. Request arrives
   - If a participant handles the request by accepting it or rejecting it, the activity ends in the corresponding state.
   - If the request times out, the system checks the **Skip Escalation** property.
2. Check for skipping escalation.
   - If **Skip Escalation** is set, the activity continues and checks the **No Timeout Action** property.
   - If **Skip Escalation** is not set, the systems checks for the escalation participant. If it can identify the configured escalation participant, the activity is put into PENDING state for the escalation participant to handle. If no escalation participant is configured for the activity or the check for the escalation participant fails, the activity ends with state TERMINATED/FAILED.

3. Check for timeout action. If **Skip Escalation** is set or the activity times out of the PENDING state for escalation, the system checks the **No Timeout Action** property.
   - If FALSE, the system proceeds and checks the **Complete On Timeout** property.
   - If TRUE, the activity is placed in PENDING state. A participant can approve or reject the request.
4. Check for what to do when the activity times out.
   - If **Complete On Timeout** is set (TRUE), the postscript for the activity runs and the activity state is set to COMPLETED/TIMEOUT.
   - If **Complete On Timeout** is not set (FALSE), the system sends a timeout notification and the activity state is set to TERMINATED/FAILED.

View activities

Use the View Activities page to view your activities, approve requests, reject requests, and complete work order activities. You can provide information for a request to proceed, approve recertification requests, reject recertification requests, and complete compliance alerts.

The View Activities page is where you view, complete, and delegate action items that are assigned to you. Action items listed in your View Activities list are part of workflow processes that require your participation before they can complete. These action items can be individual or a collection of requests for information, approvals, recertifications, work orders, or compliance alerts. You can complete the collection of items as one unit.

The View Activities page contains the following item types:

- Approval requests
- Recertification requests
- Work Order requests
- Requests for Information (RFI)
- Policy Compliance alerts

You can lock, unlock, forward, and respond to action items.

System administrators can view and respond to all user activity lists. However, system administrators cannot lock work items unless they meet the criteria of being a potential owner of the item.

Viewing activities (to-do items)

You can view a list of to-do items that require action.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. On the View Activities page, click **Refresh** to update the **Activities** table.

3. To view the details of an activity, click the activity. The information about the activity is read-only.
4. Click **Close** to close the activity details.
5. When you are done reviewing activities, click **Close**.

Viewing activities for a user

You can view a list of to-do items that require action by a specific user.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities by User**.
2. On the Select Account page, type the user ID in the **User ID** field and then click **Search**.
3. In the ITIM Accounts table, select the accounts that you want to view activities for. These activities are associated with a specific user ID and activity owner.
4. Click **Continue**.
5. On the View Activities by User page, click the activity to view information about the activity. The information about the activity is read-only.
6. Click **Close** to close the activity details.
7. When you are done reviewing activities for a user, click **Close**.

Completing an approval activity

You can approve or reject incoming to-do items.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. On the View Activities page, click the name of the approval activity.
3. On the Approval Details page, review the approval details, enter a comment for the approval or rejection of the request, and click **Approve** or **Reject**.
4. On the Success page, click **Close**.

Completing a request for information activity

You can provide information for to-do items that require additional information.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. On the View Activities page, click the name of the request for information activity.
3. On the RFI Details page, review the request for information details and click **Provide Information**.
4. On the Provide Information page, provide information for the request as needed and click **Submit**.
5. On the Success page, click **Close**.

Completing a work order activity

You can complete work order activities.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. On the View Activities page, click the name of the work order activity.
3. On the Work Order Details page, review the work order, enter any comments as needed, and click one of the following options:
   - Click **Successful** to indicate that the work order was completed successfully.
   - Click **Warning** to indicate that the work order completed successfully, but with warnings or exceptions.
   - Click **Failure** to indicate that the work order was not completed successfully.
4. On the Success page, click **Close**.

Completing a recertification activity

You can complete to-do items that require recertification.

Before you begin

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

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. On the View Activities page, click the name of the recertification activity.
3. On the Approval Details page, review the recertification, enter any comments as needed, and click **Approve** or **Reject** to approve or reject the recertification.
4. On the Success page, click **Close**.

Completing a compliance alert activity

You can correct or defer accounts or access entitlements that do not comply with a policy.

Before you begin

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

About this task

Policy compliance alerts can be displayed when accounts or access entitlements do not comply with a policy. For example, you have an existing account to use an employee records database. An administrator creates a policy that states that you must be assigned to the role of `HRManager` to access the records. To bring the account back into compliance, you must be assigned the role of `HRManager`.

You might need to defer policy compliance alerts. In the example, assume that you cannot assign the `HRManager` role to each account without first verifying that the owner of each account belongs in the role of `HRManager`. You determine that the amount of time it takes to verify that each account owner exceeds the escalation period of the alert, at which time, the alert is forwarded. You can decide to defer the compliance alert, which keeps the item in your activities list for an extended period.

You can correct or defer multiple policy compliance alerts at one time if they are grouped together in your activities list.

Policy compliance alerts listed in your activities list are part of workflow processes that require your response before they can complete.

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. On the View Activities page, click the name of the compliance alert activity.
3. On the Compliance Alert Details page, review the compliance alert, enter any comments as needed, and click one of the following options:
   - Click **Correct** to correct the compliance alert.
   - Click **Defer** to defer the compliance alert to a later time.
4. On the Success page, click **Close**.

Deferring policy compliance alerts

You can defer policy compliance alerts in your activities list.

Before you begin

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

About this task

You might need to defer policy compliance alerts in the following example. Assume that you are responsible for accounts used to access an employee records database. An administrator creates a policy that states that all accounts must be assigned to the role of `HRManager` to access the records. The accounts are currently not compliant with the policy. In order to bring the accounts back into compliance, they each must be assigned the role of `HRManager`. Now assume that you cannot

assign the HRManager role to each account without first verifying that each account owner belongs in the role of HRManager. You determine that the amount of time required to verify each account owner is greater than the escalation period of the alert. Escalation forwards the alert. You decide to defer the compliance alert, which keeps the item in your activities list for an extended period.

You can defer multiple policy compliance alerts at one time if they are grouped together in your activities list.

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. Click **Defer**.
3. On the Success page, click **Close**.

Locking an activity

You can lock activities so others cannot act on them.

Before you begin

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

About this task

Action items that are assigned to you are displayed in your activities list. In some cases, you might be only one of a collection of participants able to complete the same items. For items that are assigned to multiple people, you can select one or more activities and lock them. Use the lock to act on the item and prevent others from duplicating or otherwise conflicting with your efforts. Locked items are displayed as locked in the queues of other participants, with only the lock owner or a system administrator able to unlock them.

Lock actions are an audited process. If the lock owner is removed from the system, their locks are also removed.

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. Select one or more activities, and click **Lock** to lock the activities.

Unlocking an activity

You can unlock activities so that others can act on them.

Before you begin

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

About this task

Action items that are assigned to you are displayed in your activities list. In some cases, you might be only one of a collection of participants able to complete the same items. For items that are assigned to multiple people, you can select one or

more activities. Lock them in order to act on the item and prevent others from duplicating or otherwise conflicting with your efforts. Locked items are displayed as locked in the queues of other participants, with only the lock owner or a system administrator able to unlock them.

To unlock an activity, complete these steps:

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. Select one or more locked activities, and click **Unlock** to unlock the activities.

Assigning activities to another user

You can assign activities to other users so others can complete them.

Before you begin

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

About this task

A person can be designated as the new owner of the activity if they are a participant of the selected activity as an individual. A new owner of an activity can be a member of a relevant group, such as a service owner. For example, you might assign an activity in your queue to the queue of another person that was listed specifically as a required approver for the item.

To assign an activity to another user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Activities** > **View Activities**.
2. Select one or more activities, and click **Assign**.
3. Select an authorized user from the table, and click **Assign**. Only authorized users are displayed in this table for selection.
4. On the Success page, click **Close**.

Delegate activities

You can delegate activities to another user during a time when other users are not available to manage them.

To delegate activities from one user to another user, the user you are delegating to must have authorization from the system administrator to manage activities. If you are delegating activities for yourself, you must have both read and write Delegate access control item attribute permissions set to `Grant`. The logged-in user must have the access control item permission to write the `delegate` attribute of the user who is delegated.

You can add or delete delegation schedules for the user whose activities you are delegating. Adding a delegation schedule requires you to select a user who can manage activities and specify a time period in which to delegate activities. You can

set up multiple delegation schedules for multiple delegates, but time periods cannot overlap. If you already delegated activities and want to turn off delegation, delete the delegation schedule.

Delegation does not affect the escalation period for an activity; that is, it does not restart the countdown to the escalation date.

Creating a delegation schedule

You can delegate your to-do items to another user during a time when you are not available to manage them by creating delegation schedules.

Before you begin

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

About this task

Your activities can be delegated only to one user. Your activities might be delegated to one user. If you delegate them to another user without stopping the first delegation, the second delegation replaces the first one.

Delegation does not affect the escalation period for an activity; that is, it does not restart the countdown to the escalation date.

Procedure

1. From the navigation tree, select **Manage Activities** > **Manage Delegation Schedules**.
2. On the Manage Delegation Schedules page, click **Add** to create a delegation schedule.
3. On the Setup Delegation page, click **Search** to find a user.
4. On the Select Delegate Account page, complete these steps:
   a. Type information about a user in the **User ID** field and click **Search**.
   b. In the Accounts table, click the name of the user whose account you want to delegate your activities to, and click **OK**.
5. On the Setup Delegation page, click the calendar and clock icons to choose a date and time for starting and ending the delegation, and click **OK**.
6. On the Success page, click **Close**.

Changing delegation schedules

You can change your current delegation schedule.

Before you begin

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

About this task

If you change a delegation schedule, you are only allowed to change the schedule and not the delegation owner.

Delegation does not affect the escalation period for an activity; that is, it does not restart the countdown to the escalation date.

Procedure

1. From the navigation tree, select **Manage Activities** > **Manage Delegation Schedules**.
2. On the Manage Delegation Schedules page, select the delegation schedule you want to change and click **Change** to modify the delegation schedule.
3. On the Setup Delegation page, click the calendar and clock icons to choose a new date and time for starting and ending the delegation. Then, click **OK**.
4. On the Success page, click **Close**.

Deleting delegation schedules

You can delete or cancel delegation schedules in your to-do items.

Before you begin

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

About this task

When you delete an active delegation, you are stopping the current delegation.

Deleting a delegation does not affect the escalation period for an activity; that is, it does not restart the countdown to the escalation date.

Procedure

1. From the navigation tree, select **Manage Activities** > **Manage Delegation Schedules**.
2. On the Manage Delegation Schedules page, select the delegation schedule you want to remove, and click **Delete**.
3. On the Confirm page, click **Delete**.
4. On the Success page, click **Close**.

Chapter 14. Requests administration

The View Requests task indicates the progress and completion of submitted changes and requests that you and other users make to the system.

Request status is available through the View Requests task from the main navigation tree. You can choose to filter your search for requests by user or service. To view pending requests, click **View Requests** > **View Pending Requests by User** or **View Requests** > **View Pending Requests by Service**. You can also choose to view the status of all pending and completed requests from the **View Requests** > **View All Requests** task.

Requests

Requests are items that initiate a workflow, or work order for manual service operations, and instigate the various activities of a workflow.

There are many different types of requests that can occur, such as requesting changes to accounts, adding and modifying users, and changing policies. Some requests might require the completion of a to-do activity by another user, such as an approval or recertification. Other requests might complete without any action required.

Note: Requests that do not initiate a workflow, such as Orphan Account Requests do not get displayed in the pending or completed requests.

Requests can involve several steps to complete. Each step might require different users to complete an action. You can view the status of a request by viewing pending requests or all requests that are both pending and completed.

Completed requests are requests that completed processing. The completion of a request does not mean that it was successful. Requests might fail, might complete with a warning message, or might be canceled while in a pending state.

Pending requests are requests that are submitted but are not finished. These requests might be in the process of running or might require the completion of a workflow activity, such as a recertification or approval activity.

Request states

When you view the status of a request, the request might be in one of several states.

The states of a request can be viewed only by the user who submitted the request. The following table provides a description of each request state.

Table 99. Descriptions of the states of requests

Request state	Description
Not started	The request was not started.
In process	The request is running and is not waiting for any activity for which there is a participant.

Table 99. Descriptions of the states of requests (continued)

Request state	Description
Pending approval	The request requires approval, and no action is taken to complete the request.
Pending information	The request requires that an information provider completes a request for information (RFI) activity.
Pending response	The request requires that a responder complete a workflow activity, such as a work order or compliance alert.
Canceled	The request is canceled.
Successful	The request was completed successfully.
Completed with warning	The request was partially completed. A problem occurred, preventing the request from being successfully completed.
Failed	The request was not able to complete. No further activity can occur.

This section describes the workflow request status and its indicators and how the request status indicator works, including few examples.

Status A status of a request is associated with several child requests or processes, and each child request has a status of its own. The status of the parent request depends on the status of the child requests.

Errors An error occurs when a subsequent child request failed or was rejected. For example, when an incorrect URL is specified for reconciliation of the service or when an approver rejects a request.

Warnings

A warning occurs when one or more child requests failed. For example, you want to change passwords of five accounts simultaneously. However, even if one change password request failed and other four change password requests succeeded, the status of the parent request is `Warning`.

Note: A warning might also include activities that are marked as `Terminated`. For example, two approvers are involved in an approval workflow and none of them approve the request within the specified time period. Then the approval activity is marked as `Terminated` and the status of the parent request is `Warning`.

Success

A request is successful in one of the following situations:

- When all the child requests are successful
- When the primary child requests are successful

When the primary child requests are successful, it might also include approval activities that are marked as `Approved`. For example, two approvers are involved in an approval workflow and the first approver approves the request. In this case, the status of the approval activity is `Approved`, but the status of the parent request is `Success`.

Pending

A pending request occurs when one or more child requests are in a pending state. For example, you request to create an account that requires approval workflow. In this case, if the approval activity is pending, then the status of the parent request is also `Pending`.

Note: Pending requests might also include activities that are marked as `Escalated`. For example, a user requests an account on a service with an associated approval workflow that involves two approvers. If the first approver fails to approve the request within the specified time period, the status of the approval activity is `Escalated`. But the status of the parent request is `Pending`.

Viewing all requests

You can view all the requests that users submitted.

Before you begin

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

About this task

Use the View All Requests page to use various search criteria to find all requests are submitted to the system, regardless of their completion status.

View All Requests is only intended for users that have full, unrestricted access to the audit trail. There is no ACI checking in this view. Use caution when exposing this task in a user's view.

Procedure

1. From the navigation tree, select **View Requests** > **View All Requests**.
2. On the View All Requests page, complete these steps:
   a. Select a request type from the list.
   b. Select a time interval.
   c. Optionally, click the icon (▸) next to **More Search Criteria** to filter by status, date request was completed or submitted, service, user, or request ID.
   d. Click **Search Requests** when you are done specifying search criteria.
3. To view the details of a request, click the request type. The information about the request is read-only.
4. Click the icon (▸) below the Process Data section to view further information about the initial process data of the request.
5. On the View All Requests page, click the root structure to view the request details. The information about the request is read-only.
6. Click **Close** to close the View All Requests page.
7. When you are done reviewing the requests, click **Close**.

Viewing pending requests of users

You can view those requests that are submitted by a user, but are not completed.

Before you begin

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

About this task

Use the View Pending Requests by User page to search by user information to find requests that are submitted to the system, but are not yet completed.

View Pending Requests by User is intended for the help desk administrators and managers that need to view the audit trail related to specific users. ACIs are only applied when initially searching for a user. ACIs are not applied to any of the request data shown as a result of selecting a user.

Procedure

1. From the navigation tree, select **View Requests** > **View Pending Requests by User**.
2. On the View Pending Requests by User page, click **Search** to specify a user in the **User name** field.
3. On the Select a User page, complete these steps:
   a. Type information about the user in the **Value** field, select an attribute from the **Attribute** list, and then click **Search**.
   b. In the **Users** table, select the user whose requests you want to view.
   c. Click **OK**.
4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field, and then click **Search Requests**.
5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon (▸) below the Process Data section to view further information about the initial process data of the request.
7. On the View Pending Requests by User page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the View Pending Requests by User page.
9. When you are done reviewing the pending requests of others, click **Close**.

Viewing all requests of users

You can view all the requests that a user submitted.

Before you begin

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

About this task

Use the View All Requests by User page to search by user information to find all requests that are submitted to the system, regardless of their completion status.

View All Requests by User is intended for the help desk administrators and managers that need to view the audit trail related to specific users. ACIs are only applied when initially searching for a user. ACIs are not applied to any of the request data shown as a result of selecting a user.

Procedure

1. From the navigation tree, select **View Requests** > **View All Requests by User**.
2. On the View All Requests by User page, click **Search** to specify a user in the **User name** field.
3. On the Select a User page, complete these steps:
   a. Type information about the user in the **Value** field, select an attribute from the **Attribute** list, and then click **Search**.
   b. In the **Users** table, select the user whose requests you want to view.
   c. Click **OK**.
4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field. Optionally, filter for request status in the **Status** field, and then click **Search Requests**.
5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon (▸) below the Process Data section to view further information about the initial process data of the request.
7. On the View All Requests by User page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the View All Requests by User page.
9. When you are done reviewing the requests, click **Close**.

Viewing pending requests by service

You can view all pending requests that are submitted for a particular service.

Before you begin

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

About this task

Use the View Pending Requests by Service page to search by service information to find requests that are submitted to the system, but are not yet completed.

View Pending Requests by Service is intended for service and application owners that need to view the audit trail related to services they administer. ACIs are only applied when initially searching for a service. ACIs are not applied to any of the request data shown as a result of selecting a service.

Procedure

1. From the navigation tree, select **View Requests** > **View Pending Requests by Service**.
2. On the View Pending Requests by Service page, click **Search** to specify a service in the **Service name** field.
3. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Service information** field. Select a service type from the **Service Type** list and then click **Search**.
   b. In the **Services** table, select the service whose requests you want to view.
   c. Click **OK**.

4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field and then click **Search Requests**.
5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon (▸) below the Process Data section to view further information about the initial process data of the request.
7. On the View Pending Requests By Service page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the View Pending Requests by Service page.
9. When you are done reviewing the requests for a service, click **Close**.

Viewing all requests by service

You can view all the requests that are submitted for a particular service.

Before you begin

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

About this task

Use the View All Requests by Service page to search by service information to find all requests that are submitted to the system, regardless of their completion status.

View All Requests by Service is intended for service and application owners that need to view the audit trail related to services they administer. ACIs are only applied when initially searching for a service. ACIs are not applied to any of the request data shown as a result of selecting a service.

Procedure

1. From the navigation tree, select **View Requests** > **View All Requests by Service**.
2. On the View All Requests by Service page, click **Search** to specify a service in the **Service name** field.
3. On the Select a Service page, complete these steps:
   a. Type information about the service in the **Service information** field, select a service type from the **Service Type** list, and then click **Search**.
   b. In the **Services** table, select the service whose requests you want to view.
   c. Click **OK**.
4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field. Optionally, filter for request status in the **Status** field, and then click **Search Requests**.
5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon (▸) below the Process Data section to view further information about the initial process data of the request.
7. On the View All Requests By Service page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the View All Requests by Service page.

9. When you are done reviewing the requests for a service, click **Close**.

Canceling pending requests

You can cancel requests that are not completed.

Before you begin

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

About this task

Pending requests are requests that are submitted to the system, but are not yet completed. When a pending request is canceled, the request is canceled. Any action items associated with the request are canceled and the request status is changed to canceled.

Note: When you cancel a request, the workflow is interrupted and is not fully processed.

Administrators can also choose to search for requests to cancel from the navigation tree by selecting **View Requests** > **View Pending Requests by Service** and **View Requests** > **View Pending Requests by User**.

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

Procedure

1. From the main navigation tree, click **View Requests** > **View All Requests**.
2. On the View All Requests page, complete these steps:
   a. Click the icon (▸) next to **More Search Criteria**.
   b. Under Status, clear all items except **Pending**.
   c. Optionally, you can filter by date, service, and user to narrow your options.
   d. Click **Search Requests** to display a list of pending requests.
   e. Select the request that you would like to cancel, and click **Cancel Request**.
3. On the Confirm page, click **Cancel Requests**.
4. On the Success page, click **Close**.

Results

When a request is canceled, an email notification is sent to the requester, provided that:

- Notification is not disabled. (By default, notification is enabled.)
- The email server and other properties are configured in the `enroleMail.properties` file.
- The requester has a valid email address.

The email notification lists the person who canceled the request, the date and time that the request was canceled, and the reason that the request was canceled.

Related tasks:

"Manually applying the email notification template changes for canceling a request" on page 419
You can use the Workflow Notification Properties page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.3, the email notification template content that includes information about canceling a request is not automatically applied. The template changes that are available with Fix Pack 6.0.0.3 are not automatically applied so that the installation process does not overwrite any custom changes that you might have made to the email templates.

Related reference:

"Request for information (RFI) states" on page 443
When you view the status of a request, the request for information (RFI) activities might be in one of several states.

Index

A

access
  clearing from service instance 170
  configuration, namespace 294
  configuration, query items 295
  configuration, query subjects 294
  deleting 45
  management 43
  overview 43
  requesting 44
  type, creating, based on role 110
  viewing 45
access audit
  history, reports 211
  namespace 290
  query items 291
  query subjects 290
  report models 207
access audit (Deprecated)
  namespace 285
  query items 286
  query subjects 285
access control
  overview 77
  reports 201
access control items
  administrator domains 67
  changing 84
  creating 83
  default 77
  definition 77
  deleting 85
access data
  CSV
    formats 90, 126, 179
    values 90, 126, 179
access definition
  filters 209
  report, base icon URL path 217
access information
  configuring for a group 185
  configuring for a role 101
  configuring for a service 129
access reports, defining 203
account
  audit history, reports 211
  audit, namespace 235
  audit, query items 236
  audit, query subjects 235
  changing details 40
  configuration, namespace 239
  configuration, query items 241
  defaults, adding to service 153
  defaults, changing 154
  defaults, global 157
  defaults, management 152
  defaults, removing from service 156
  management on a service 141
  status filters 210
  types 37
  viewing details 40
account information
  modifying 144
account information, editing 144
account recertification
  displaying status 166
  overview 166
accounts 37
  active, inactive 37
  adding default values 153
  assigning users 149
  changing 144
  changing defaults in a service 144
  deleting 41, 145
  displaying 142
  editing 144
  modifying 144
  orphan 150
  overview 37, 141
  policy enforcement 372
  recertification overview 166
  recertification, displaying status 166
  report models 206
  requesting 38, 143
  restoring 42, 148
  suspending 41, 146
  viewing 39
ACIs
  administrator domains 67
  changing 84
  creating 83
  default 77
  deleting 85
  report filters 347
  reports 346
activities
  administration overview 441
  approval 441, 448
  assigning 452
  compliance 444
  compliance alert 450
  deferring compliance 450
  definition 441
  delegate 50, 452
  delegating 51
  delegating, changing schedule 453
  delegating, creating schedule 453
  delegating, overview 50, 452
  delegating, stopping 454
  locking 451
  overview 50, 452
  recertification 383, 444, 449
  request for information 442, 448
  RFI 448
  to-do list 445
  unlocking 451
  viewing 447
  viewing user 448
  work order 443, 449
activity reminder in workflow 416
administration
  creating nodes, organizational tree 68
administration *(continued)*
  organization 67
administrator
  access restriction 201
  domains, ACIs 67
adoption
  changing policies 353
  creating policies 350
  deleting policies 354
  orphan account policies 355
  policies
    attribute matching 354
  policies overview 349
  policies, JavaScript examples 351
  policy reconciliation 355
  writing policies 351
aliases 29
application interfaces
  management 15
approvals
  activities 441
  completing 448
  states 442
approveSoDViolation 396
assignment attributes 96
  defining for existing role 99
  defining when creating role 98
  setting values 100
attribute matching 354
attributes 29, 299
  defining assignment for existing role 99
  defining assignment for new role 98
  mapping 299, 325
  unmapping 326
audit
  and security, generating 313
  history report 210
  report, example 320
authentication
  IBM Cognos reports 198
authorization 77
  IBM Cognos reports 198

C

cancel request
  notification template 419
changelog 341
child roles
  adding to parent role 108
  managing 106
  removing from parent role 109
Cognos Business Intelligence
  installation 193
comma-separated value file
  reconciliation 139
compliance alert rules, configuring 164
connection mode
  changing 124
  enabling 120

console reports
IBM Security Identity Manager 308
content store, creation 194
conventions 342
CSV
data values, formats 90, 126, 179
CSV file
reconciliation 139
custom reports
creating 314
generating 317
shared access objects 318
custom tables, adding 301
custom tasks
changing 75
changing task parameters 75
defining access 73
deleting 76
customization
model 301
password age rules 370
password rules 366
adding customized password generator 367
adding customized rule 366
customized rules and generator 368
report banner 335
reports 314

D

dashboard
IBM Security Identity Manager environment 213
data source
IBM Security Identity Manager Cognos reports 196
data synchronization 193
creating a schedule 338
deleting a schedule 340
modifying a schedule 339
overview 336, 337
synchronizing data immediately 338
db2admin 64
changing password 65
db2inst1 64
default values, accounts 153
define base icon URL path
access definition report 217
delegation schedules
changing 453
creating 453
deleting 454
domain administrator, creating 68
draft provisioning policies 378
drill-through reports 197

E

email response objects 27
enabling connection mode 120
entities 299
mapping 299
mapping attributes 299
entitlements
report filters 212
environment variables settings 195
escalation 445
period in workflow 417
event log
view 13
events
SNMP 25
example
accounts, filters 332
audit report check-in 320
checking out shared access credentials 318
filters 333
person and organization roles 333
persons and account, filters 334
role and shared access entitlement 322

F

filters
access definition 209
account status 210
accounts 332
custom reports 332
entitlements report 212
persons and account 334
separation of duty policy definition 214
services report 215
fix pack, installation 7
Framework manager
configuration 194
IBM Cognos 191
installation 193

G

global account defaults 157
globalization, language support 204
groups 29
access information 185
adding members 175
administration overview 173
configuring manual service type 138
creating 173
defining access on 184
deleting 183
enabling automatic membership 188
exporting access data 180
importing access data 181
modifying attributes 178
recertifying access on 187
removing members 177
viewing members 174

H

hosts
files 18

I

IBM Cognos
components 301
connection 191
installation prerequisites, report models 191
objects, report models 205
prerequisites, report models 191
report server, software requirements 192
reporting framework 190
IBM Security Identity Manager 213
Cognos reports troubleshooting 305
Cognos reports, data source 196
console reports 308
identities 356
identity
creating policies 358
definition 356
deleting policies 360
policies 355
policies, changing 360
policies, creating 358
policies, deleting 360
policies, overview 355
policies, script 356
Incremental Data Synchronizer
changelog 341
conventions 342
overview 340
starting 342
starting, command interfaceIncremental Data Synchronizer 343
starting, graphical user interface 342
tuning 344
ISIM Environment dashboard
editing 195
refresh interval 195
itimuser 64
changing password 65

J

JOIN conditions, design reports 334
join directive 371

L

language preferences, setting 205
language support, globalization 204
LDAP
creating users 200
LDAP namespace
configuration 198
ldapdb2 64
ldapdb2, changing password 66
log response objects 27
login
administration 53
overview 53
setting maximum attempts 53
logs 27

M

management
  hosts files 18
management, account defaults 152
management, reconciliation
  schedules 131
manual connection mode
  creating a service 117
manual services
  changing 125
  creating 121
members, adding 202

N

namespace
  access audit 290
  access audit (Deprecated) 285
  access configuration 294
  account audit 235
  account configuration 239
  provisioning policy audit 248
  provisioning policy
    configuration 251
  recertification audit 218
  recertification configuration 228
  report models 205
  role audit 255
  role configuration 258
  separation of duty audit 265
  separation of duty configuration 271
  service audit 281
  user configuration 273
node tree
  administering 67
  changing 69
  creating 68
  deleting 69
notification
  escalation in workflow 416
  in workflow, disabling 418
  in workflow, enabling 418
notification for passwords 61
notification template
  cancel request 419
notifications 25, 27

O

object
  email 27
  log 27
objects 27
organization
  administration 67
  changing a node 69
  creating a node 68
  deleting a node 69
  node tree 67
organizational roles
  access information 101
  adding users to membership 104
  administration 87
  assignments 96
  child, adding to parent role 108
  child, managing 106
organizational roles *(continued)*
  child, removing from parent role 109
  classifying 93
  creating 89
  creating access type 110
  deleting 102
  displaying role-based access 95
  exporting access data 91
  importing access data 92
  managing users as members 103
  modifying 89
  overview 87
  removing users from
    membership 105
  specifying owners 94
orphan accounts
  account reconciliation 355
  making 150
  overview 150
overview
  data synchronization 336
  format 189
  incremental data synchronizer 340
  report data synchronization
    utility 344
  reports 189

P

packages, publishing 301
parameter enforcement rules 373
password
  policies 361
password age rules
  configuration 369
password policies
  changing 364
  creating 362
  definition 361
  deleting 366
password policy
  adding targets 363
  changing rules 365
  changing targets 364
  creating rules 363
password rules, customized logic 368
password strength rules 61, 361
passwords
  adding minimum password age 370
  administration of system settings 55
  administration overview 55
  changing 46, 48
  changing for db2admin 65
  changing for itimuser 65
  changing for ldapdb2 66
  configuring administrator-defined
    questions for 62
  configuring minimum password
    age 369
  creating strength rules 61
  customized rules 366, 369, 370
    adding customized logic 368
    adding customized password
      generator 367
    adding customized rule 366
  enabling editing 57
  enabling resetting 55
passwords *(continued)*
  excluding 63
  expiration 53
  forgotten 62
  hiding generated 56
  management 46
  resetting 47, 49
  setting on user creation 59
  setting retrieval expiration 60
  setting the notification method 61
  showing generated 57
  synchronization 58
pending requests
  viewing by service 459
  viewing by users 457
person and organization roles filters 333
person profiles 29
policies
  adoption 349
    changing 353
    creating 350
    deleting 354
  approving 405
  changing identity 360
  creating identity 358
  definition 349
  deleting identity 360
  enforcing 165
  identity 355
  password 361
    changing 364
    creating 362
    deleting 366
  provisioning 371
    changing 375
    creating 374
    deleting 378
    preview 376
  recertification 380
    changing 391
    creating 387, 388, 389
    default notifications 392
    deleting 391
    results 385
  separation of duty 394, 396, 405
    ACI operations 395
    changing 401
    creating 400
    default ACI 396
    deleting 403
    disabled 394
    enabled 394
    enabling the portfolio task 399
    evaluating 402
    exemptions 397, 404
    revoking exemptions 406
    violations 397, 404
  service selection
    change 409
    create 408
    delete 410
    overview 408
policy enforcement
  compliance alerts 159
  configuring enforcement 162
  definition 372
  overview 159

policy enforcement *(continued)*
policy enforcement actions 159
policy enforcement alerts 159
scheduling on service 165
policy evaluation 397
policy management 349
portfolio tasks 399
provisioning
policies 371
report models 206
provisioning policies
changing 375
creating 374
definition 371
deleting 378
draft
change 378
commit 378
create 377
managing by role 379
parameter enforcement rules 373
preview 376
provisioning policies draft, creating 377
provisioning policy audit
namespace 248
query items 250
query subjects 248
provisioning policy configuration
namespace 251
query items 252
query subjects 252

Q

query items 218
access audit 291
access audit (Deprecated) 286
access configuration 295
account audit 236
account configuration 241
provisioning policy audit 250
provisioning policy configuration 252
recertification audit 220
recertification configuration 229
role audit 256
role configuration 260
separation of duty audit 267
separation of duty configuration 272
service audit 282
user configuration 274
query studio 191
query subjects 218
access audit 290
access audit (Deprecated) 285
access configuration 294
account audit 235
account configuration 239
provisioning policy audit 248
provisioning policy configuration 252
recertification audit 218
recertification configuration 228
role audit 255
role configuration 258
separation of duty audit 266
separation of duty configuration 271
query subjects *(continued)*
service audit 281
user configuration 273

R

recertification
account 166
activities 383
completing 449
message templates 383
notification 383
overview 444
report models 206
schedule 383
recertification audit
namespace 218
query items 220
query subjects 218
recertification configuration
namespace 228
query items 229
query subjects 228
recertification definition
access 214
account 214
subreports 214
user 214
recertification policies
changing 391
creating 387, 388, 389
default notifications 392
deleting 391
overview 380
results 385
reconciliation 355
changing a schedule 136
creating a schedule 135
deleting a schedule 137
deleting reconciliation schedule 137
managing schedules 131
manual service overview 138
overview 131, 133
reconciling accounts immediately 134, 138
references
mapping entities 299
security configuration 204
regular expression notation, searching 313
relationship
creating 301
modifying 301
with existing tables, creating 302
reminder interval in workflow 417
removing account defaults 156
report
server execution mode 194
shared access entitlement creation 322
report banner customization 335
report data synchronization utility
overview 344
run 345
running 345
troubleshooting errors 346
report generation 304
report models 205
access audit 207
accounts 206
IBM Cognos objects 205
provisioning 206
recertification 206
roles 207
separation of duty 207
services 207
users 207
report package
defining access 203
importing 196
report parameters and descriptions
access approval and rejection 208
audit, account 208
noncompliant account 208
shared access, entitlements by owner 208
shared access, entitlements by role 208
report studio 191
reporting framework
reporting model 190
static reports 190
reports
access audit history 211
access control 201
access control items 346, 347
account audit history 211
ACI 346
adhocreporting.properties 336
audit and security 313
audit history report 210
configuration files 336
custom 317
custom reports 332
customization 314
DatabaseFunctions.conf 336
define access 203
delete custom templates 317
deleting custom templates 317
designing, JOIN conditions 334
drill-through 197
filters 332
format 189
generate 311, 317
generating 311, 312, 313
mapping attributes 325
modify custom templates 316
modifying custom templates 316
overview 189
requests 311
schema mapping 325
separation of duty policy violation 215
services 312
synchronizing data 337, 338, 339, 340
templates 314
types 308
unmapping attributes 326
user and accounts 312
user input filters 329
user input values 327
user recertification history 217
request for information
completing 448

request for information *(continued)*
overview 442
states 443
requests
accounts 143
cancelling 461
definition 445, 455
generating 311
overview 445, 455
states 455
view all 457
view all by service 460
view pending 457
view pending by service 459
viewing 455
viewing all by service 460
viewing all submitted by user 458
response objects
email 27
log 27
SNMP 25
restoration, accounts 148
retry blocked request 114
RFI overview 442
role audit
namespace 255
query items 256
query subjects 255
role configuration
namespace 258
query items 260
query subjects 258
role custom report templates
creating 324
roles 29, 87, 96
adding users to membership 104
assignment attributes 96
child, adding to parent role 108
child, managing 106
child, removing from parent role 109
classifying 93
creating 89, 202
creating access type 110
deleting 102
displaying role-based access 95
exporting access data 91
hierarchies 88
importing access data 92
managing users as members 103
modifying 89
removing users from membership 105
report models 207
specifying owners 94
rules
compliance alert, configuring 164
configuring, password 369
customized logic, password 368
customizing password age rule 370
customizing, password 366

S

sample workflow
access owner approval 438
approval loop 428
mail activity 430
sample workflow *(continued)*
manager approval of accounts 420
multiple approvals 421
multiple approvals with loop 424
packaged approval 434
RFI and subprocess 427
sequential approval for user recertification 431
scenario
adding custom tables 301
creating a relationship 302
customize model 301
generating report 304
schedules, delegating 51
schema mapping 218
reports 325
script, identity policy 356
search, regular expression notation 313
security administration overview 71
security configuration references 204
security layer configuration 198
separation of duty audit
namespace 265
query items 267
query subjects 266
separation of duty configuration
namespace 271
query items 272
query subjects 271
separation of duty policies 396
ACI operations 395
changing 401
creating 400
default ACI 396
definition, filters 214
deleting 403
disabled policy 394
enabled policy 394
enabling the portfolio task 399
evaluating 402
exemptions 397, 404
exemptions, revoking 406
overview 394
violation, reports 215
violations 397, 404
violations, approving 405
separation of duty report models 207
server monitoring
management 10
service
access information 129
changing 123
clearing access 170
creating 115
creating, manual connection mode 117
managing access 169
managing accounts on 141
managing groups 169
status 114
tagging 158
service audit
namespace 281
query items 282
query subjects 281
service selection policies
changing 409
service selection policies *(continued)*
creating 408
deleting 410
overview 408
service tags, adding 159
service template, adding tag attribute 158
service types
default 112
overview 112
services
deleting 131
exporting access data 127
generating 312
importing access data 128
manual, changing 125
manual, creating 121
policy enforcement 372
reconciling accounts 134, 135, 136, 137, 138
report filters 215
report models 207
viewing all requests 460
viewing pending requests 459
set of tasks 71
setup, user authentication 198
shared access configuration 194
shared access credentials, example 318
shared access objects
custom reports 318
simple network management protocol (SNMP) 25
snapshots, management 21
SNMP monitoring
management 14
software requirements
IBM Cognos report server 192
sponsored accounts
changing passwords 48
resetting passwords 49
static reports, IBM Cognos models 191
static routes
management 19
support files, management 23
suspension, accounts 146
syslog 27
system audit events
configuration 24
system users
db2admin 64
db2inst1 64
default 64
itimuser 64
ldapdb2 64
passwords 64

T

tag attribute, adding 158
tagging, service 158
tags, adding to service 159
TCR reports
migrating to IBM Cognos reports 301
migration to IBM Cognos reports 301
templates, reports 314
to-do lists 445

troubleshooting
IBM Security Identity Manager Cognos reports 305
report data synchronization utility 346
tuning 344
types, reports 308

U

user accounts
deleting 41
requesting 38
restoring 42
suspending 41
user activities, viewing 448
user and accounts, generating 312
user authentication
setup 198
user configuration
namespace 273
query items 274
query subjects 273
user input
filters, reports 329
values, reports 327
user passwords
changing 46, 48
resetting 47, 49
user profiles
changing 32
creating 30
deleting 33
user information, changing 32
user recertification
history, reports 217
users 29
adding to membership of role 104
administration overview 29
assigning to accounts 149
creating 30
delegating activities 51
deleting 33
deleting access 45
managing as members of role 103
removing from membership of role 105
report models 207
requesting access 44
requesting accounts for 38
restoring 35
suspending 34, 36
transferring 34
viewing access 45
viewing accounts for 39
viewing activities for 448
viewing all requests submitted 458

V

view 71
changing 72
changing custom tasks 75
creating 71
defining custom tasks 73
deleting 73
view *(continued)*
deleting custom tasks 76
View activities page 447
virtual appliance
system settings, manage 5
virtual appliance dashboard 1
administrator settings, manage 21
date and time, manage 20
firmware settings, management 6
manage about page 7
manage CPU usage 9
manage memory usage 8
manage storage usage 10
restart or shutdown 28
update history, manage 5
viewing cluster status 4
viewing disk usage 1
viewing IP addresses 2
viewing licensing 6
viewing middleware monitor widget 3
viewing notifications 2
viewing partition information 1
viewing quick links 3
viewing server control 3

W

web gateway configuration 194
web server configuration 194
work order
states 443
work orders
activities 443
completing 449
workflows
adding 411
changing 412
deleting 413
disable 418
enabling 418
escalation period 417
mail activity template 413
management overview 411
notification 418, 419
notification, activity reminder 416
notification, escalation 416
reminder content in workflow 417
reminder interval 417
sample, access owner approval 438
sample, approval loop 428
sample, mail activity 430
sample, manager approval of accounts 420
sample, multiple approvals 421
sample, multiple approvals with loop 424
sample, packaged approval 434
sample, RFI and subprocess 427
sample, sequential approval for user recertification 431
template 419

Printed in USA