

IBM Security Privileged Identity Manager
Version 2.0.1

Administrator Guide



IBM Security Privileged Identity Manager
Version 2.0.1

Administrator Guide



Note

Before using this information and the product it supports, read the information in Notices.

Edition notice

Note: This edition applies to Version 2.0.1 of *IBM Security Privileged Identity Manager* (product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2013, 2015.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures vii

Tables ix

Chapter 1. Appliance Dashboard 1

Viewing notifications	1
Viewing the cluster status	1
Viewing and using server controls	3
Viewing deployment statistics	3
Viewing the middleware and server monitor widget	3
Viewing and using quick links	4
Viewing disk usage	4
Viewing IP addresses	4
Viewing partition information	5
Viewing the update history	5
Viewing the licensing	5
Managing the firmware settings	6
Installing a fix pack	7
Viewing the About page information	7
Viewing the memory utilization	8
Viewing the CPU utilization	9
Viewing the storage utilization	9
Configuring the date and time settings	10
Configuring the administrator settings	10
Managing the snapshots	11
Managing the support files	12
Restarting or shutting down	12

Chapter 2. User administration 13

User management	13
Creating user profiles	14
Changing user profiles	15
Deleting user profiles	16
Transferring users	16
Suspending users	17
Restoring users	17
Requesting access for users	18
Password management	18
Changing user passwords	18
Resetting user passwords	19
Delegate activities	20
Delegating activities for another user	20

Chapter 3. Login administration 21

Enabling password expiration	21
Setting a maximum number of login attempts	21

Chapter 4. Password administration . . 23

Enabling password resetting	23
Hiding generated reset passwords	24
Showing generated reset passwords	24
Enabling password editing and changing	25
Enabling password synchronization	25
Setting a password when a user is created	26

Setting a password retrieval expiration	27
Creating password strength rules	27
Enabling forgotten password authentication	27
Configuring user-defined forgotten password questions	28
Configuring administrator-defined forgotten password questions	29
Excluding specific passwords	29

Chapter 5. Organization administration 31

Administrator domains	31
Making a user a domain administrator	32
Creating a node in an organization tree	32
Changing a node in an organization tree	33
Deleting a node in an organization tree	33

Chapter 6. Shared access administration 35

Credential vault management	35
Creating a privileged administrator	36
Credentials in the credential vault	36
Viewing credentials in the credential vault	40
Modifying credentials in the credential vault	41
Registering credential passwords in the credential vault	44
Viewing password history for credentials in the credential vault	46
Removing credentials from the credential vault	47
Checking in credentials from a credential vault	48
Fields for Advanced search for credentials	48
Specifying non-exclusive shared access credentials	49
Credential management	49
Adding credentials through Manage Credentials	49
Modifying credentials	51
Deleting credentials	51
Checking in credentials	52
Resetting credential password	52
Connecting a credential to an identity provider	52
Disconnecting a credential from an identity provider	54
Configuring scheduled password reset	54
Configuring a lifecycle rule for rotating passwords	54
Credential pool management	55
Creating credential pools	55
Deleting credential pools	56
Modifying credential pools	57
Viewing credentials in the pool	58
Checking in credentials in a credential pool	59
Resource management	61
Adding resources	61
Modifying resources	62
Deleting resources	62
Identity provider management	62

Adding identity providers	63
Modifying identity provider	63
Deleting identity providers	64
Access administration	64
Creating access	66
Changing access	68
Shared access bulk load	68
Shared access bulk load operations	68
Format of the shared access CSV file	69
Credential matching for the #Credentials type	88
Credential matching for the #Credentials_v2 type	88
Uploading a CSV file with the administrative console	88
Configuring the credential default settings	89
Checkout operation customization	91
Define a checkout operation with the checkout extension	91
Define a checkout operation with an RFI node followed by the checkout extension	92
Changing the operation name label	93
Shared access approval for adding credentials to the vault	93
Customizing the checkout form	93
Configuring the shared access credential usage prompt	94
Configuring the reauthentication prompt	95

Chapter 7. Services administration. 97

Service types	97
Service status	100
Creating identity feed services	100
Setting the service unique identifier	101
Customizing the service form template to include the unique identifier (eruri) attribute	102
Changing identity-feed services	103
Deleting identity-feed services	104
Creating service types	105
Changing service types	106
Importing service types	107
Deleting service types	108
Reconciliation for manual services	108
Creating a reconciliation schedule	109
Changing a reconciliation schedule	110
Deleting a reconciliation schedule	111

Chapter 8. Group administration 113

Creating groups	113
Adding members to groups	114
Removing members from groups	114
Modifying groups	115
Deleting groups	116

Chapter 9. Policy administration 119

Password policies	119
Creating a password policy	119
Creating a password policy rule	120
Changing a password policy	121
Changing a password policy rule	121
Deleting a password policy	122
Customized password rules	122

Creating a user policy template only for privileged identity management users	128
---	-----

Chapter 10. Workflow management 129

Adding an entitlement workflow	129
Changing an entitlement workflow	130
Deleting an entitlement workflow	130
Creating a mail activity template with the workflow designer	131
Workflow notification properties	132
Configuring the workflow escalation period	133
Configuring the work item reminder interval and reminder content	134
Enabling workflow notification	134
Disabling workflow notification	135
Changing a workflow notification template	135
Manually applying the email notification template changes for canceling a request	135
Sample workflows	136
Sample workflow: multiple approvals	136
Sample workflow: multiple approvals with loop processing	139
Sample workflow: RFI and subprocess	142
Sample workflow: approval loop	143
Sample workflow: mail activity	145
Sample workflow: access owner approval	146

Chapter 11. Activity administration 149

Approval activities	149
Approval states	150
Request for information activities	150
Request for information (RFI) states	151
Work order activities	151
Work order states	151
To-do lists	152
Requests	152
Escalation	153
View activities	153
Viewing activities (to-do items)	153
Viewing activities for a user	154
Completing an approval activity	154
Completing a request for information activity	154
Completing a work order activity	154
Locking an activity	155
Unlocking an activity	155
Assigning activities to another user	155
Delegate activities	156
Creating a delegation schedule	156
Changing delegation schedules	157
Deleting delegation schedules	157

Chapter 12. Requests administration 159

Requests	159
Request states	159
Viewing all requests	161
Viewing pending requests of users	161
Viewing all requests of users	162
Canceling pending requests	163

Chapter 13. Session recording administration 165

Recording policies	165
Accessing recordings	165
Logging on to the IBM Privileged Session Recorder console	165
Searching for recordings	165
Saving frequently used search queries	166
Recording Permalink	166
Playing back recordings	167
Customizing the columns displayed	168
Database archival	168
Archiving the database	169
Restoring an archived recording	170
Adding a partition set	171

Chapter 14. Application identity management. 173

Providing managed credentials to a script	176
Providing managed credentials to data source connections for WebSphere Application Server applications	177
Providing managed credentials to a Java application	179
Application identity management tasks.	180
Registering an Application Instance	180
Granting an application access to shared credentials on resources	182
Managing the list of authorized applications	183

Chapter 15. Report administration 185

References	186
Report model configuration by using IBM Cognos components	186
Scenarios	186
Report descriptions and parameters	188
Application ID Registration Report	188
Application Instance Activity Audit Report	188
Shared Access Entitlement by Owner Report	189
Shared Access Entitlement by Role Report	189
Shared Access Entitlement Definition Report	190
Shared Access History Report	190
Single Sign-On Privileged ID Audit Report	191
Privileged Session Recorder Report	191
Report models	192
Single Sign-On Module model.	193
Shared Access Management model	193
Application ID Module model.	193
Report schema mapping.	193
Mapping attributes	194
Unmapping attributes	194
Data synchronization	195
Data synchronization for reports	196
Incremental data synchronizer overview	199
Utility for external report data synchronization	203
Query subjects and query items for the report models	204

Mapping the attributes and entities	204
Single Sign-On Audit namespace for Single Sign-On Module	205
PSR Audit namespace for Single Sign-On Module	207
Audit namespace for shared access module	208
Configuration namespace for shared access module	213
Application ID Configuration namespace for Application ID Module	221
Application Instance Activity Audit namespace for Application ID Module	223
Generating the report through IBM Cognos Business Intelligence	225

Chapter 16. Security administration 227

View management.	227
Creating a view	227
Changing a view	228
Deleting a view	228
Defining a custom task	229
Changing a custom task	230
Deleting a custom task	232
Access control item management	232
Default access control items	233
Creating an access control item	234
Changing an access control item	235
Deleting an access control item	236

Chapter 17. Deprecated tasks 237

Role administration	237
Role overview	237
Role hierarchy change enforcement	238
Creating roles	238
Modifying roles	238
Values and formats for CSV access data (role)	239
Exporting access data for a role	240
Importing access data for a role	241
Classifying roles	242
Specifying owners of a role.	243
Displaying a role-based access in the user interface	244
Role assignment attributes	245
Deleting roles	250
Managing users as members of a role	251
Adding users to membership of a role	252
Removing users from membership of a role	253
Managing child roles	254
Adding child roles to a parent role	255
Removing child roles from a parent role	256
Creating an access type based on a role	256
Shared access policy management	257
Creating shared access policies	257
Modifying shared access policies	260
Deleting shared access policies	260

Notices 263

Figures

1. Privileged administrators grant users access to resources with a simplified entitlement model	65	5. Sample workflow: approval loop	144
2. Sample workflow: multiple approvals required	137	6. Sample workflow for access request	146
3. Sample workflow: multiple approvals with loop processing	139	7. Playback and view controls	167
4. Sample workflow: RFI and subprocess	142	8. Application identities are often embedded inside data sources, custom applications, or unattended scripts to retrieve sensitive information.	173

Tables

1. Synchronization states table.	2	27. Filters for the Single Sign-On Privileged ID Audit Report.	191
2. Data reference for shared access.	35	28. Filters for the Privileged Session Recorder Report.	192
3. Identity providers for managed resources.	63	29. Single Sign-On Module model namespaces	193
4. Equivalent legacy role for each access assignment type	65	30. Shared Access Management model namespaces	193
5. Person attributes for an LDAP filter	67	31. Application ID Module model namespaces	193
6. Password entry options	94	32. Definitions for directory variables.	200
7. Node properties: Sample workflow for multiple approvals.	137	33. Parameters and arguments for the Incremental Data Synchronizer script	202
8. Node properties: Sample workflow for multiple approvals with loop processing	139	34. Specifying the location of the Java runtime environment	203
9. Node properties: Sample workflow with an RFI and a subprocess	142	35. Mapping the attributes and entities	205
10. Node properties: Sample workflow with an approval loop	144	36. Query subjects in the Single Sign-On Audit namespace	206
11. Node properties: Sample workflow for access request.	147	37. Query items in the Single Sign-On Audit namespace	206
12. Descriptions of the states of approval activities	150	38. Query subjects in the PSR Audit namespace	207
13. Descriptions of the states of RFIs	151	39. Query items in the PSR Audit namespace	208
14. Descriptions of the states of work order requests	152	40. Query subjects in the Audit namespace	208
15. Descriptions of the states of requests	159	41. Query items in the Audit namespace	209
16. What you can search for in recordings	165	42. List of query subjects in the Configuration namespace	213
17. Advanced playback and view controls	167	43. Query items in the Configuration namespace	214
18. Properties that can be used for fingerprinting with different application types.	174	44. List of query subjects in the Application ID Configuration namespace	221
19. Custom Properties	179	45. Query items in the Application ID Configuration namespace	222
20. Basic tasks to configure report model	186	46. List of query subjects in the Application Instance Activity Audit namespace	223
21. Filters for the Application ID Registration Report	188	47. List of query items in the Application Instance Activity Audit namespace	224
22. Filters for the Application Instance Activity Audit Report.	188	48. Default access control items for Shared Access Module	233
23. Filters for Shared Access Entitlement by Owner Report	189	49. CSV fields and values.	239
24. Filters for Shared Access Entitlement by Role Report	189	50. Part 1 of 2: Role access CSV file values, formats	240
25. Filters for the Shared Access Entitlement Definition Report	190	51. Part 2 of 2: Role access CSV file values, formats	240
26. Filters for Shared Access History Report	190		

Chapter 1. Appliance Dashboard

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

Viewing notifications

You can view warning information about potential problems and required actions with the **Notification** dashboard widget.

Procedure

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

Identity service restart required
SingleSignOn service restart required
SessionRecorder service restart required
Appliance restart required
Middleware components not configured
The disk space utilization has exceeded the warning threshold.
Synchronize the current Member node with the Primary node.
Reconnect the current Member node with the Primary node.

2. Take the appropriate actions, as required. For example:

If the following warning messages are displayed, restart the identity service by using the option that is provided in the **Server Control** widget.

Identity service restart required
SingleSignOn service restart required
SessionRecorder service 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.

Viewing the cluster status

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.

The Cluster Status widget is displayed only when you are in a cluster setup. In a 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 of the node in the cluster. For more information, see the following table.

Table 1. Synchronization states table.

State	Description	Action
Not Connected	Displays when a Member node cannot connect to a Primary node or when a Primary node cannot connect to the Member node.	Connect the Member node with the Primary node. For a node with the Not Connected status, click Reconnect Node to connect that node into the cluster. See Reconnecting a node into the cluster.
Not Synchronized	Displays when the Member node is not synchronized with the Primary node.	Synchronize the Member node with the Primary node. See Synchronizing a Member node with a Primary node.
Synchronized	Displays when the Member node is synchronized with the Primary node.	No action is required.
Synchronizing	Displays when the Member node is synchronizing with the Primary node.	Wait until the synchronization is complete. Click the Refresh icon to get the most recent status.

Table 1. Synchronization states table. (continued)

State	Description	Action
Not Applicable	Displays if the cluster node is a Primary node because the Primary node does not require any synchronization.	No action is required.
Error	Displays when the action fails to retrieve synchronization details for the node.	Check log files for more information.

- Optional: Click the **Refresh** icon to display the updated data again.

Viewing and using server controls

You can view the status and control different components in the system by using the **Server Control** widget.

Procedure

- From the **Appliance Dashboard**, locate the **Server Control** widget.
- Do one of the following actions:
 - Stop** Stops all the server components.
 - Start** Starts all the server components.
 - Restart**
 - Restarts the server as per the requirement.
- Optional: Click **Refresh** to display the data again.

Viewing deployment statistics

You can view information about number of users, groups, services, credentials, and credential pools in the system by using the **Deployment Statistics** widget.

Procedure

- From the **Appliance Dashboard**, locate the **Deployment Statistics** widget. The first row displays the type of entity. The second row displays the number of entities that exist in the system.
- Optional: Click **Refresh** to display the data again.

Viewing the middleware and server 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 and Server Monitor** dashboard widget.

Procedure

- From the **Appliance Dashboard**, locate the **Middleware and Server Monitor** widget.
- Optional: Click **Refresh** to display the data again.

Viewing and using quick links

You can view the links for accessing the administration console application. This option is provided mainly for an appliance Administrator to validate the success of IBM® Security Privileged Identity Manager configuration.

About this task

You can view the **Quick Links** widget only on a stand-alone node.

Procedure

1. From the **Appliance Dashboard**, locate the **Quick Links** widget. The various links are as follows:
 - Identity and Credential Vault Administration
 - Single Sign-On and Session Recorder Administration
 - Session Replay Console
2. Click a quick link to view and use for your requirement.

Viewing disk usage

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

Procedure

1. From 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.

Consumed Disk 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 Disk Space

Displays how much space (in GB) is available.

Total Disk 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 data again.

Viewing IP addresses

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

Procedure

1. From the **Appliance Dashboard**, locate the **Interfaces** widget. The IP address is displayed.
 2. Optional: Click **Refresh** to display the data again.
-

Viewing partition information

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

Procedure

1. From 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, 2.0.

Installation date

Displays the date on which the virtual appliance firmware was installed. For example, Dec 5, 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 5, 2014 8:19:40 PM.

2. Click **Firmware Settings** to go the page to modify settings of the firmware.
-

Viewing the update history

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

About this task

After you install an update, the update package is deleted from the IBM Security Privileged 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.
 2. Optional: Click **Refresh** to display the data again.
-

Viewing the licensing

View the licensing to see the service agreement that you accepted when you installed the IBM Security Privileged Identity Manager virtual appliance.

About this task

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

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Licensing**. The Licensing page is displayed.
2. Click **Service Agreement** to view the service agreement in the Software License Agreement page.

Managing the firmware settings

The IBM Security Privileged 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 Privileged 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 Privileged Identity Manager virtual appliance restarts the system by using partition 2, which is now the active partition.

Note: The IBM Security Privileged 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.
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 Privileged 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 Privileged 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 Privileged 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 the fix pack file.
4. Select the fix pack file, and click **Open**. The Browse for fix pack table displays the fix pack details.
5. Click **Save Configuration** to install the fix pack.

Viewing the About page information

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

Procedure

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

Results

The following information is displayed in the About page:

Product Name: IBM Security Privileged Identity Manager
Product Version: 2.0
Server Name: ispmva.example.com
Installed Fix Packs: None
Build number: 20141205-1328
Build Date and Time: Dec 5, 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 Privileged Identity Manager virtual appliance product information to determine how it can be useful in your work.

Viewing the memory utilization

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

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Graphs > 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 three 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 seven 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 **Memory Used** to review the total used memory.

Viewing the CPU utilization

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

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Graphs > 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 three 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 seven 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.

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.

Viewing the storage utilization

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

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Graphs > 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 three days. Each data point is an average of the activity that occurred in that hour.

Option	Description
7 Days	Displays data points every 20 minutes during the last seven 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.

- In the Legend area, select which partitions that you want to review.

Boot Indicates the boot partition.

Root Indicates the base file system, where the system user is root.

Configuring 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 Privileged Identity Manager virtual appliance.

Procedure

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

Option	Description
Date	Specifies the day, month, and year for the IBM Security Privileged Identity Manager virtual appliance.
Time	Specifies the time for the IBM Security Privileged Identity Manager virtual appliance.
Time Zone	Specifies the time zone for the IBM Security Privileged Identity Manager virtual appliance.
NTP Server address	Select Enable NTP to list the NTP (NIST Internet Time Service) servers that the IBM Security Privileged 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 SiteProtector™ System console. You can specify only NTP server addresses.

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

Configuring the administrator settings

Use the administrator settings to change the password that you use to access your IBM Security Privileged 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 Privileged Identity Manager virtual appliance.

About this task

Snapshots are stored on the IBM Security Privileged 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, click New , type a comment to describe the snapshot, and then click Submit .
Edit	To edit the comment for a snapshot, select the snapshot, click Edit , type a new comment, and then click Submit .
Delete	To delete snapshots, select one or more snapshots, and then click Delete .
Apply	To apply a snapshot, select the snapshot, and then click Apply . Note: 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 migrated to the current firmware version.
Download	To download a snapshot, select the snapshot, click Download , browse to the drive where you want to save the snapshot, and then click Save . Note: If you download multiple snapshots, the snapshots are compressed into a .zip file.
Upload	To upload snapshots, click Upload , browse to the snapshots you want to upload, select the snapshots, and then click OK . Note: You can upload only one snapshot at a time.
Refresh	To refresh the list of snapshots, click Refresh .

Managing the support files

IBM Customer Support uses support files to help you troubleshoot problems with the IBM Security Privileged 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, click New , type a comment to describe the support file, and then click Submit . A new support file is created on the IBM Security Privileged Identity Manager virtual appliance.
Edit	To edit the comment for a support file, select the support file, click Edit , type a new comment, and then click Submit .
Delete	To delete a support file, select the support file, and then click Delete .
Download	To download support files, select the support files, click Download , browse to the drive where you want to save the support files, and then click Save . Note: If you download multiple support files, the files are compressed into a .zip file.

Restarting or shutting down

Use the Restart or Shutdown page to restart or shut down the IBM Security Privileged 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 Privileged Identity Manager virtual appliance takes it offline for several minutes.
Shut Down	Shutting down the IBM Security Privileged 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 built-in system accounts and access in IBM Security Privileged Identity Manager.

The built-in system accounts for a person include the IBM Security Privileged Identity Manager account and the IBM Security Access Manager for Enterprise Single Sign-On agent account. The built-in system accounts are automatically created when a person is created and automatically removed when a person is removed.

Use the Manage Users page for these tasks.

User management

A *user* is a person with IBM Security Privileged Identity Manager account. Users perform their required tasks in the IBM Security Privileged Identity Manager.

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 that is 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 role is a method of providing users with access to the managed credentials and credential pools. Organizational roles determine which credentials and pools are granted for a user or set of users who share similar responsibilities.

If a user is assigned to an organizational role, the credentials and credential pools that are granted to the role, through shared access policy, are accessible to the user.

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. A role might be a child role of multiple organizational roles.

Groups

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

Some users might belong to default groups that IBM Security Privileged 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 Privileged Identity Manager user profile for an individual who requires one.

Before you begin

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

Procedure

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

1. From the navigation tree, select **Manage Users**.
2. On the Select a User page, click **Create**.
3. 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 IBM Security Privileged 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 access.

Changing user profiles

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

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**.

Deleting user profiles

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

About this task

When you delete a user, all the accounts that are associated with the user are deleted as well.

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 name of the user you want to delete. You can select one or more users to delete.
 - c. 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**.

Transferring users

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

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 Privileged Identity Manager, you can suspend the system access that the user has.

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. 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.

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 you want to restore.
 - c. 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.

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

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

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. Click **Submit** to complete the request, or click **Schedule Submission** to select a date and time to schedule the request.
5. On the Success page, click **Close**.
6. On the Select Access page, click **Close**.

Password management

There are two ways to manage passwords in IBM Security Privileged 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.

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.

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.
 - 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.

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.

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.

- 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**.

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.

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 Privileged Identity Manager passwords within a specified time period.

Before you begin

Note: If you configured IBM Security Privileged Identity Manager to use the default custom registry, you can 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.

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

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.

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 Privileged 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 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 Privileged Identity Manager.

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

Enabling password resetting

Users or administrators with the correct permissions can *reset* users' passwords to new passwords that are generated by IBM Security Privileged Identity Manager. Alternatively, depending on the password settings of IBM Security Privileged 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.

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.

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.

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.

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 Privileged 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.

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.

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 Privileged Identity Manager. Alternatively, depending on the password settings of IBM Security Privileged 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.

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.

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 accounts that a user owns. Password synchronization reduces the number of passwords that a user must remember. Password synchronization does not affect sponsored accounts.

About this task

You can configure the system to automatically synchronize passwords for all accounts that are owned by a user. Then, the user must remember only one password.

Note: When password synchronization is enabled, IBM Security Privileged Identity Manager does the ACI evaluation for changing password on the person entity. If the person ACI grants the user the change password operation, the user can change the password for all associated accounts.

If password synchronization is enabled, users cannot specify different passwords for their accounts.

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 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

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 Privileged Identity Manager satisfies these criteria for IBM Security Privileged Identity Manager Server login accounts. A user that is created through the user interface is automatically provisioned an Security Privileged 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 IBM Security Privileged 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 ISPIM service service type that sets erpassword during auto-provisioning to the value stored in the person record.

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.

About this task

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.

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**.

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

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

Procedure

1. From the navigation tree, select **Manage Password Policies**.
2. Create a password policy or change an existing one. Ensure that you selected an identity provider 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 Privileged Identity Manager password and must reset it, the user must verify credentials with the system.

About this task

You can configure IBM Security Privileged Identity Manager to present either administrator-defined questions or user-defined questions. You can also define how many questions must be answered.

Note: This task is effective only if a WebSphere® account repository is specified. This field is on the ISPIM service **Manage Services > Change a Service > Service Information** page. This repository can be ISPIM service or a service managed by

the IBM Security Privileged 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 questions 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.

- If you do not predefine the questions, the user must specify both the forgotten password questions and the answers.
- If you predefine the forgotten password questions, the user must specify only the answers.

If the system configuration changes, for example, from undefined questions to predefined questions, the user must specify answers to the new questions.

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.

Configuring user-defined forgotten password questions

You can enable and configure forgotten password settings to allow users to supply their own questions for challenge response authentication.

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 **Enforce password change and log in to system** if you want users to change the password and log in to the system 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 **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.
 - c. In the **Challenge Behavior** field, click the radio button next to **Users define their own questions**.
 - d. Type in the number of questions the user must set up and answer correctly to successfully authenticate, and click **OK**.
3. On the Success page, click **Close**.

Configuring administrator-defined forgotten password questions

You can enable and configure forgotten password settings to set predefined questions for challenge response authentication.

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 **Enforce password change and log in to system** if you want users to change the password and log in to the system 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 **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.
 - c. In the **Challenge Behavior** field, click **Administrator provides predefined questions**.
 - d. Click the arrow icon next to **Specify Forgotten Password Question** to expand it.
 - e. Type in a challenge question, select a locale for the question, and click **Add**. Repeat this process as necessary when you are adding more than one question.
 - f. Select a choice for whether the user has a choice of predefined questions. These options are displayed:
 - **No, answer all questions** - The user must answer all predefined questions to be authenticated.
 - **Yes, user selects which questions to answer** - The user can select which predefined questions to answer. You are prompted to enter a number for how many predefined questions the user must set up.
 - **No, answer a subset of questions that the system provides** - To authenticate, the user must set up one or more predefined questions from a subset of challenge questions. The user must provide a specified number of correct answers.
 - g. 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.

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.

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

Any IBM Security Privileged 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 IBM Security Privileged Identity Manager administrator or an IBM Security Privileged Identity Manager user. The user has rights to add, modify, or delete an admin domain through ACIs.

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 Privileged Identity Manager user as the administrator of an administrator domain. The IBM Security Privileged 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.

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.

About this task

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

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

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.

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. Shared access administration

The Shared Access Management provides centralized management of shared and privileged accounts. It enables sharing credentials among multiple users.

You can store its credentials (user ID and password) in a credential vault. Access to these credentials is governed by a role-based shared access policy.

You can group credentials that have a similar level of access privileges into a *credential pool*. A credential tag is used to represent the level of access privilege. A credential pool defines a credential tag or a set of credential tags. Credentials that meet the pool definition become members of the pool. An authorized user can request to check out a credential. The system selects an available credential from the pool and checks it out for the user.

When multiple credential tags are specified for a credential pool, only the credentials with all those tag values are resolved as the pool members.

A shared access policy authorizes role members to share credentials or credential pools. A policy can be defined for:

- A specific credential pool
- A specific credential
- For all pool or credentials with the same organization container context

Table 2 describes data references that you can use during administration tasks.

Table 2. Data reference for shared access

Data Reference	Description
"Default access control items" on page 233	Use the default access control items for shared access to manage access security.
Shared access tables	IBM Security Privileged Identity Manager creates and uses these database tables to store information related to Shared Access Management. .
Shared access classes	Shared Access Management has several types of object classes, such as credential component, credential, credential pool, credential lease, and shared access policy. The credential and credential pool are considered as credential component and both inherit the same shared attributes of the <code>erCredentialComponent</code> class.
Auditing schema tables	You can use auditing schema to track credential management, credential pool management, credential lease management, and shared access policy management. The audit event schema has a common base event table, <code>audit_event</code> , which contains fields common to all audit events.

Credential vault management

As a privileged administrator, you can add credentials for resources to the credential vault so that they can be shared with other users.

A *credential vault* is a repository that holds the credentials (user IDs and passwords) for shared accounts and resources.

Before working with the credential vault, make a user a privileged administrator. See “Creating a privileged administrator.”

Note: The best practice is to make a user a privileged administrator so that the user has all the ACIs needed to work with the credential vault. It is suggested that this privileged administrator be an administrator of an Admin Domain. As a domain administrator, all ACIs that are needed to manage all entities in the domain are present. If you do not use an Admin Domain, you might need to complete additional ACI setup to grant control over roles, credentials, credential pools, and shared access policies.

Creating a privileged administrator

A privileged administrator can manage and delegate the activities that are shown in the administrative console view for the privileged administrator group. The Privileged Administrator group can also view nearly all tasks on the self service console.

Procedure

1. If it does not exist, create a user profile for the user that you want to be the privileged administrator. For information, see “Creating user profiles” on page 14.
2. If the Admin domain in which you want the user to be a privileged administrator does not exist, create it. Make the user an administrator for the domain, with permissions for that domain and any domains below it. For information, see the following topics:
 - “Making a user a domain administrator” on page 32
 - “Administrator domains” on page 31
3. Click **Manage Users**. On the Select a User page, search for the user you created, or click **Refresh** on the table to display users.
4. Click the icon (▶) beside the name of the user you created, and click **Accounts**. The Accounts page is displayed.
5. Click **Refresh** on the **Accounts** table to display the accounts for the user.
6. Click the user ID in the row where the **Service Name** is **ITIM Service**. The Account Information page is displayed.
7. Click **Search**. The Select Groups page is displayed.
8. Click **Search**. Groups are displayed in the **Groups** table.
9. Select the check box beside the **Privileged Administrator** group, and click **OK**. The Account Information page is displayed, with **Privileged Administrator** displayed in the **Groups** field.
10. Click **Submit Now** or **Schedule Submission**.
11. Click **Close** on the Success page.

Credentials in the credential vault

Credentials in the credential vault can be connected to an account or not connected to an account.

Credentials that are connected to an account

Privileged administrators can add credentials that are connected to an existing account to the credential vault.

To add credentials that are connected to an account to the credential vault, select **Manage Shared Access > Manage Credential Vault** in the administrative console. See Adding credentials that are connected to an account through Manage Credential Vault.

When you add a credential that is connected to an account to the credential vault, you can choose to have the password for the credential and account on the managed resource updated automatically when the user checks in the credential.

Credentials that are not connected to an account

Privileged administrators can add credentials that are not connected to an account to the credential vault. You can select **Manage Shared Access > Manage Credential Vault** in the administrative console. See “Adding credentials through Manage Credential Vault.”

There are advantages of adding credentials to the credential vault in this way:

- You do not need to first create a service and run reconciliation to get shared accounts in IBM Security Privileged Identity Manager.
- You do not need to provide as much information as when you add a credential that is connected to an account. You provide only information about the user ID and some information about the resource to which the user ID applies. For example, if you know about a user account on a UNIX system, you can add the credentials for that system to the credential vault. Other IBM Security Privileged Identity Manager users can then check out the credentials and use them to access the UNIX system.

However, when you add a credential that is not connected to an account to the credential vault, you cannot have the password updated automatically when the user checks in the credential.

Adding credentials through Manage Credential Vault

As a privileged administrator, you can add credentials of managed resources into the credential vault. Other users can check out and use these credentials; however, when a user checks in these credentials, the password does not change.

You can share these credentials with other users even if you have limited information. For example, you might know only the user ID, password, and some information (such as the IP address) that uniquely identifies the resource. You can add the credentials to the credential vault with only this information.

Before you begin

To add credentials to the credential vault, you must have the authority to administer shared credentials under your domain or organizational unit. The privileged administrator has this authority.

Depending on how your system administrator customized your system, you might not have access to this task. Ask your system administrator to make you a privileged administrator so that you can have access to this task.

As a privileged administrator and a domain administrator, you have access control items (ACIs) for the protection categories of Credential and Credential Service. For more information about ACIs, see “Access control item management” on page 232.

About this task

Adding the credentials for a resource to the credential vault enables the credentials to be shared.

Procedure

To add credentials to the credential vault without connecting them to an account, complete the following steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The Select a Credential page is displayed.
2. On the Select a Credential page, complete these steps:
 - a. Optional: Click **Refresh** in the Credentials section of the page to display credentials that are currently in the credential vault.
 - b. Click **Add**. The Select Options for Credentials page is displayed.
3. On the Select Options for Credentials page, complete these steps:
 - a. Select the type of sharing for this credential. The option that you choose determines whether the credential is shared and whether it must be checked out and checked in by users. You can select from the following options:

Use default setting

Select this option if you want to use the default settings for your system for sharing credentials.

The current default setting is displayed below the list of sharing options.

Share a credential that requires checkout

Select this option if you want to share the credential with other users, who must check out the credential to use it. If you select this option, only one user at a time can check out the credential.

Share a credential that does not require checkout

Select this option if you want to share the credential with other users, who do not need to check out the credential before they use it. If you select this option, more than one user can use the credential at a time.

Store a credential for sharing later

Select this option if you do not want to share the credential now, but you want to store it in the credential vault.

- b. Click **Continue**.

The Credential notebook is displayed.

4. On the General page of the Credential notebook, complete these steps:
 - a. If you are authorized to add credentials to only one business unit, that business unit is displayed in the **Business Unit** field. If there are many business units to which you can add credentials, check to see whether the business unit that is displayed is the one in which you want to add the credential. If it is not, click **Search**. Find the correct business unit and add it to the **Business Unit** field.
 - b. Type the user ID for the credential in the **User ID** field. For example, the user ID might be marybeth on a UNIX system.
 - c. Optional: In the **Description** field, type information about the credential that you want to add to the credential vault. For example, you might type Shared credential for using the department UNIX system.

- d. Optional: Type the password for the credential in the **Password** and **Confirm Password** fields. If the password is not specified for the credential, the credential will not be available for checkout.

Note: IBM Security Privileged Identity Manager does not validate the password. If you enter the wrong password, the accounts are not accessible when they are checked out. The administrator must modify the credentials in the credential vault before they can be accessed.

- e. Specify the time interval, in days, for password reset.
- f. Assign a credential tag.
- g. In the **Resource Information** section, click **Search** to locate a resource for the credential. A resource consists of resource UID, resource name, and optionally, resource alias, and resource tag. The Select Resource page is displayed.
- h. On the Select Resource page, click **Search** to locate an existing resource. To limit the search results, you can type information in the **Resource UID or alias** or **Resource Name** field, or in both fields. The search results are displayed in the **Resource** table.
- i. View the search results, and take one of the following actions:
 - If the resource that you want to use for the credential exists and you want to use it without changing it, select it in the **Select** column, and then click **OK** to return to the General page.
 - If the resource does not exist, click **New** in the **Resource Information** table. The Specify Information page is displayed.
 - If the resource for the credential exists and you want to change it (for example, resource aliases or resource tags), click **Change**. The Specify Resource Information page is displayed.

Note: If another credential uses the resource that you modify, the resource for the other credential that uses this resource is affected. Be careful if you use this function.

- j. If you clicked **New** or **Change**, complete the following fields on the Specify Information page:

Resource UID

Type information that uniquely identifies the resource for which you are adding credentials. This field identifies the repository on which this user ID is hosted. For example, the unique identifier might be the IP address or the URL of a host or application.

Resource Name

Type a common name for the resource for which you are adding credentials to the credential vault. This common name identifies the repository on which this user ID is hosted. For example, the name might be Department UNIX system.

Resource Alias

Optional. Type a resource alias and click **Add**. You can specify multiple resource aliases.

The resource alias is used if you also use IBM Security Access Manager for Enterprise Single Sign-On for automatic checkout. The resource alias is the IP address or hostname of the managed resource to which the credential applies. IBM Security Access Manager for Enterprise Single Sign-On uses the resource alias and the resource UID to locate the resource.

To remove a resource alias, select the alias in the list and click **Delete**.

Resource Tag

Optional. Enter a resource tag for the managed resource and click **Add**. You can specify multiple resource tags.

To remove a resource tag, select the resource tag in the list and click **Delete**.

Click OK.

The General page is displayed with the resource displayed in the Credential Service Information table.

5. Optional: On the Credential Setting page of the notebook, view the following fields.

Default Settings

This section is displayed if you selected **Use default setting** on the Select Options for Credentials page. The default settings that were configured by the system administrator are displayed. You cannot change these fields.

Default Access Mode

Require the checkin and checkout process for shared IDs.

Maximum checkout duration

If this field is displayed, specify the number of hours, days, or weeks for which the credential can be checked out.

Operation Name

Enable check out search

If this check box is displayed, select the check box if you want to enable the credentials for a checkout search.

Display password to user

If this check box is displayed, select the check box if you want to display the credential password to the user on the Self Service user interface.

6. Optional: On the Justification page of the notebook, provide reasons in the **Justification** field for adding the credential to the credential vault.
7. Click **Submit**. The Success page is displayed, confirming that your request to add credentials to the credential vault is successfully submitted.

What to do next

Create a shared access policy. This role-based policy entitles members of roles to share credentials.

See “Creating shared access policies” on page 257.

Viewing credentials in the credential vault

As a privileged administrator, you can view the settings for credentials in the credential vault.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of **Credential**. For more information about ACIs, see “Access control item management” on page 232.

About this task

You can use this task to view the checkin and checkout settings for account credentials in the credential vault.

Note: If you do not have authorization to modify the settings, the settings are read-only.

Procedure

To view the credentials in a credential vault, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The **Select a Credential** page is displayed.
2. Click **Search** to locate the credentials that you want to view. If you do not specify any additional information, the search includes all login IDs and services in the credential vault. To limit the scope of the search, complete these steps:
 - a. In the **Login ID** field, specify a login ID associated with the credentials. For example, type `bsmith`.
 - b. Enter a specific resource name in the **Resource name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all resources that contain that term in the name.
 - c. Optional: Click **Advanced**. The advanced search option opens a new page where you can specify additional search criteria. For information about the Advanced search fields, see “Fields for Advanced search for credentials” on page 48.

The credentials that match the search criteria are displayed in the **Credentials** table.

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. Click the hyperlink of the credential that you want to view. The General page of the Credential notebook is displayed with information about the credential.
 4. When you finish viewing the credential information, click **Cancel**.

Modifying credentials in the credential vault

As a privileged administrator, you can modify the credentials in the credential vault.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of **Credential**. For more information about ACIs, see “Access control item management” on page 232.

About this task

You can use this task to change information for credentials in the credential vault.

Note: If you do not have authorization to modify the information, the fields are read-only.

Procedure

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The Select a Credential page is displayed.
2. Click **Search** to locate the credentials that you want to view. If you do not specify any additional information, the search includes all login IDs and services in the credential vault. To limit the scope of the search, complete these steps:
 - a. In the **Login ID** field, specify a login ID associated with the credentials. For example, type `bsmith`.
 - b. Enter a specific resource name in the **Resource name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all resources that contain that term in the name.
 - c. Optional: Click **Advanced**. The advanced search option opens a new page where you can specify additional search criteria. For information about the Advanced search fields, see “Fields for Advanced search for credentials” on page 48.

The credentials that match the search criteria are displayed in the **Credentials** table.

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. Select the check box next to the credential that you want to modify.
 4. Click **Change**. The General page of the Credential notebook is displayed.
 5. Optional: On the General page of the Credential notebook, change any of the following fields:

User ID

The User ID for the credential.

Description

Type information about the credential.

Credential Service Information table

The credential service consists of service UID, service name, and optionally, a service type and one or more service aliases. In addition, there might be one or more service tags. To change the information, click **Search**. The Select Credential Service page is displayed. Complete the following steps:

- a. On the Select Credential Service page, click **Search** to locate the credential service. To limit the search results, you can type information in the **Resource UID or alias** or **Resource Name** field, or in both fields. The search results are displayed in the **Credential Service Information** table.
- b. View the search results, and take one of the following actions:

- If the resource that you want to use for the credential exists and you want to use it without changing it, select it in the **Select** column, and then click **OK** to return to the General page.
- If the resource does not exist, click **New** in the **Resource Information** table. The Specify Information page is displayed.
- If the resource for the credential exists and you want to change it (for example, resource aliases or resource tags), click **Change**. The Specify Resource Information page is displayed.

Note: If another credential uses the resource that you modify, the resource for the other credential that uses this resource is affected. Be careful if you use this function.

- c. If you clicked **New** or **Change**, complete the following fields on the Specify Credential Service Information page:

Resource UID

Type information that uniquely identifies the resource for which you are adding credentials. This field identifies the repository on which this user ID is hosted. For example, the unique identifier might be the IP address or the URL of a host or application.

Resource Name

Type a common name for the resource for which you are adding credentials to the credential vault. This common name identifies the repository on which this user ID is hosted. For example, the name might be Department UNIX system.

Resource Alias

Optional. Type a resource alias and click **Add**. You can specify multiple resource aliases.

The resource alias is used if you also use IBM Security Access Manager for Enterprise Single Sign-On for automatic checkout. The resource alias is the IP address or hostname of the managed resource to which the credential applies. IBM Security Access Manager for Enterprise Single Sign-On uses the resource alias and the resource UID to locate the resource.

To remove a resource alias, select the alias in the list and click **Delete**.

Resource Tag

Optional. Enter a resource tag for the managed resource and click **Add**. You can specify multiple resource tags.

To remove a resource tag, select the resource tag in the list and click **Delete**.

Click OK.

6. Optional: On the Credential Setting page of the notebook, change any of the following fields:
 - a. To change the credential vault setting, select one of the following settings. These settings govern the checkin and checkout process for the accounts.

Use default settings

Select this option to use the global settings. The global settings are

established by the system administrator. The configuration settings are displayed in the default settings list.

Require the checkin and checkout process for shared IDs

Select this option if you want authorized users to access the credential through the checkout process. This selection enforces individual accountability. You can specify for how long the account can be checked out.

Do not require the checkin and checkout process for shared IDs

Select this option if you want authorized users to view the password and access the credential without checking it out of the credential vault. This selection does not provide individual accountability.

Credential is not shared

Select this option if you do not want any user to access the credential by using a shared access policy. When you select this option, the credential is stored in the credential vault. However, these credentials are not available for check out.

- b. If the **Change password upon checkin** check box is displayed, select the check box if you want the password to be changed on the account and the managed resource when the user checks in the credential. If you do not want the password to be changed when the credential is checked in, clear the check box. Selecting this check box provides the best security.
 - c. If the **Maximum checkout duration** check box is displayed, specify the number of hours, days, or weeks for which the credential can be checked out.
 - d. If the **Enable checkout search** check box is displayed, select the check box if you want to enable the credentials for a checkout search. If the account is not searchable, the account cannot be checked out directly. This check box is active if the checkin and checkout process is required or the checkin and checkout process is enabled in the default settings.
 - e. If the **Display password to user** check box is displayed, select the check box if you want to display the credential password to the user on the Self Service user interface.
7. Click **Submit**.
 8. On the Success page, click **Close**.

Registering credential passwords in the credential vault

As a privileged administrator, you can register a password for one or more credentials that are added to the credential vault without a password. If the password of an account was changed on the managed resource, you can update the password in the credential vault.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of **Credential**. For more information about ACIs, see “Access control item management” on page 232.

About this task

Use this task to assign a password to one or more credentials that are stored in the credential vault. If the credential does not have a password in the credential vault,

users cannot check out the credential. If there is not a password in the credential vault for the credential, this task sets a password. If a password is changed on the managed resource, use this task to reset the password in the credential vault so that the password in the credential vault matches the password on the resource.

Note: This password must match the password on the managed resource. IBM Security Privileged Identity Manager does not verify password validity. If the password you assign does not match the password on the managed service, the credential cannot access the managed resource. If you register more than one credential with the same password, all of those credentials must have the same password on the managed resource.

Procedure

To register credentials in the credential vault, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The Select a Credential page is displayed.
2. Click **Search** to locate the credentials that you want to view. If you do not specify any additional information, the search includes all login IDs and services in the credential vault. To limit the scope of the search, complete these steps:
 - a. In the **Login ID** field, specify a login ID associated with the credentials. For example, type `bsmith`.
 - b. Enter a specific resource name in the **Resource name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all resources that contain that term in the name.
 - c. Optional: Click **Advanced**. The advanced search option opens a new page where you can specify additional search criteria. For information about the Advanced search fields, see “Fields for Advanced search for credentials” on page 48.

The credentials that match the search criteria are displayed in the **Credentials** table.

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. Select the check box next to one or more credentials for which you want to register a password.

Note: If you select more than one credential, all selected credentials must have the same password on the managed service.

4. Click **Register Password**. The Confirm page is displayed for registering the password.
5. In the **Password** field, type the password that you want to assign to the credentials.

Note: This password must match the password for the user IDs on the managed service.

6. In the **Confirm Password** field, type the password again to confirm the password.
7. Click **Submit**.
8. On the Success page, click **Close**.

Viewing password history for credentials in the credential vault

As a privileged administrator, you can view the history of passwords that are registered for a credential in the credential vault.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of **Credential**. For more information about ACIs, see “Access control item management” on page 232.

About this task

You can view the list of previously registered passwords. The passwords that are displayed do not include the current password. Therefore, if you view the password history for a new credential, the list of passwords is empty because a new credential has only a current password.


Procedure

To view the list of previously registered passwords for the selected credentials, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The **Select a Credential** page is displayed.
2. Click **Search** to locate the credentials that you want to view. If you do not specify any additional information, the search includes all user IDs and services in the credential vault. To limit the scope of the search, complete these steps:
 - a. In the **User ID** field, specify a user ID associated with the account credentials. For example, type `bsmith`.
 - b. Enter a specific service name in the **Service name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all services that contain that term in the name.
 - c. Optional: Click **Advanced**. The advanced search option opens a new page where you can specify additional search criteria. For information about the Advanced search fields, see “Fields for Advanced search for credentials” on page 48.


The credentials that match the search criteria are displayed in the **Credentials** table.

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. Locate the row in the **Credentials** table that contains the credential for which you want to view password history.
 4. In the **Name** column, hover your cursor over the  icon to display the action menu and select **View Password History**.

Note: You do not need to select the check box for the credential in the **Select** column.

The **View Password History** panel is displayed.

5. View the password entries for the credential by clicking the  icon in one of the following rows:
 - **Date** sorts the entries by date.

- **Password** sorts the entries in ascending or descending alphabetical order.
6. When you finish, click **Close** to exit the panel. The Manage Credential Vault panel is displayed.

What to do next

Perform administrative actions on other credentials or click **Close**.

Removing credentials from the credential vault

As a privileged administrator, you can remove credentials from the credential vault.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of **Credential**. For more information about ACIs, see “Access control item management” on page 232.

About this task

This task removes credentials from the credential vault. The credentials are also removed automatically from all shared access policies that reference them. If all credentials referenced by a policy are deleted by this operation, the entire policy is also deleted.

Procedure

To remove credentials from the credential vault, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The **Select a Credential** page is displayed.
2. Click **Search** to locate the credentials that you want to view. If you do not specify any additional information, the search includes all login IDs and services in the credential vault. To limit the scope of the search, complete these steps:
 - a. In the **Login ID** field, specify a login ID associated with the credentials. For example, type `bsmith`.
 - b. Enter a specific resource name in the **Resource name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all resources that contain that term in the name.
 - c. Optional: Click **Advanced**. The advanced search option opens a new page where you can specify additional search criteria. For information about the Advanced search fields, see “Fields for Advanced search for credentials” on page 48.

The credentials that match the search criteria are displayed in the **Credentials** table.

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. Select the check box next to one or more credentials that you want to remove.
 4. Click **Delete**.
 5. On the Confirm page, click **Delete**. The Success page is displayed, indicating that the delete operation was successful.

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

Checking in credentials from a credential vault

As a privileged administrator, you can check in a credential that either you or any other user checked out from a credential vault.

Before you begin

Ensure that you have the following permission: Checking in a credential on behalf of others.

Procedure

To check in credentials that are checked out, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Vault**. The Select a Credential page is displayed.
2. Click **Search** to locate the credentials that you want to view. If you do not specify any additional information, the search includes all login IDs and services in the credential vault. To limit the scope of the search, complete these steps:
 - a. In the **Login ID** field, specify a login ID associated with the credentials. For example, type `bsmith`.
 - b. Enter a specific resource name in the **Resource name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all resources that contain that term in the name.
 - c. Optional: Click **Advanced**. The advanced search option opens a new page where you can specify additional search criteria. For information about the Advanced search fields, see “Fields for Advanced search for credentials.”

The credentials that match the search criteria are displayed in the **Credentials** table.

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 **Credentials** table, select one or more credentials that you want to check in.
 4. Click **Check In**. A confirmation page is displayed.
 5. On the Confirm page, specify the date and time for the checkin to occur.
 6. Click **Check In**, or click **Cancel**. A message is displayed, indicating that you successfully checked in the credential.

Note: If the credentials that you are checking in are not connected to an account, the credential password is not changed at checkin even if the default configuration settings specify that **Change password upon checkin** is enabled.

7. Click **Close** to exit credential vault management.

Fields for Advanced search for credentials

You can limit the scope of the search for credentials by doing an advanced search.

Specify any of the following fields to limit the scope of your search.

Note: The credentials might not be associated with an account. The **Ownership type**, **Account type**, and **Owner** fields can be used only when you search for credentials that are associated with an account.

User ID

The user ID associated with the credentials. For example, specify bsmith. The search includes credentials that are associated with the user IDs bsmith, bsmith1, and bsmith2.

Business unit

Click **Search** beside this field to find the available business units.

Resource Name

Limits the search to a set of services. Type the string on which you want to search. For example, typing AIX returns AIX Service and AIX Pistons. You can also use a wildcard to search for service names that end in the string. For example, typing * service returns AIX Service and Winlocal Service. The default selection is to search all services.

Status The default setting is to search all credentials in the vault. You can limit the search to credentials that are either checked in and available or checked out and unavailable.

Specifying non-exclusive shared access credentials

Take the following steps to configure the non-exclusive credential setting for a shared access account.

Procedure

1. Start the IBM Security Privileged Identity Manager self-service interface.
2. Select **Manage Shared Access > Manage Credential Vault**.
3. Click **Refresh**.
4. Select a credential that you want to define as a non-exclusive credential.
5. Select the **Credential Setting** tab.
6. Select **Do not require the checkin and checkout process for shared IDs**. For more information about the other credential settings, see “Modifying credentials in the credential vault” on page 41.

Credential management

As a privileged administrator, you can add credentials and connect it to an identity provider so they can be shared with other users.

Adding credentials through Manage Credentials

As a privileged administrator and the domain administrator, you can add credentials.

Before you begin

Ensure that you selected the domain where you want to add the credentials.

About this task

IBM Security Privileged Identity Manager does not provision privileged credentials on target systems. The privileged credentials must already exist on the target system and added separately.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Credentials**.
2. Click **Add**.
3. On the Add Credentials page, complete these fields:

Login ID

Type the login ID for the credential. For example, a login ID might be bsmith, bsmith1, or bsmith2

Password

Type the password for the login ID.

Confirm password

Type the password again for confirmation and click **OK**.

Resource

Add a new resource or select an existing resource that you want to associate with the credential. Click **OK**.

- To associate your credential to an existing resource, select from the resource list.
- To add a resource, click the **Add** icon and complete these fields:

Resource name

Type a name for the resource for which you are adding credentials. This name identifies the repository on which the login ID is hosted. This is used for searching credentials and can be used to link the credential to a policy.

Resource Alias

Type the IP address or host name of the managed resource to which the credential applies.

Description

Type information about the credential that you want to add. For example, you might type Shared credential for using the department UNIX system.

Credential Tag

Type a tag and click the **Add** icon. You can add one or more tags to group credentials with the same characteristics. These tags are used for managing credential pools. After adding the tags, click **OK**.

Credential Settings

Select from the following settings and click **OK**.

Use default setting

Select this option if you want to use the default settings for your system for sharing credentials.

The current default setting is displayed below the list of sharing options.

Share a credential that requires checkout

Select this option if you want to share the credential with other users, who must check out the credential to use it. If you select this option, only one user at a time can check out the credential.

Share a credential that does not require checkout

Select this option if you want to share the credential with other

users, who do not need to check out the credential before they use it. If you select this option, more than one user can use the credential at a time.

Store a credential for sharing later

Select this option if you do not want to share the credential now, but you want to store it.

Password Reset Interval (Days)

Type or select an interval, in days, in which the credential password is automatically changed. The default value of 0 indicates that the credential password is not automatically changed.

4. Click **Add** to display additional row where you can add more credentials.
5. Click **Save**.

What to do next

Connect the credential to an identity provider.

Modifying credentials

As a privileged administrator, you can modify the credentials.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Credentials**.
2. Click the **Search** icon to locate the credentials that you want to view. If you do not specify any additional information, the search includes all credentials in your domain. To limit the scope of the search, you can search by login ID, description, and resource name. You can also limit your search to checked out credentials by using the **Filter By** option.
3. Select one or more credentials that you want to modify.
4. Click **Edit**. The Edit Credentials page is displayed.
5. Change the fields that you want to edit.
Modified fields are marked with a change bar on the left of side of the field. Click **Hide changes** to hide the change bars.
6. Click **Save**.

Deleting credentials

As a privileged administrator, you can delete credentials in your domain. Deleting the credentials means that the credential cannot be shared.

About this task

This task deletes credentials in your domain. The credentials are also removed automatically from all shared access policies that reference them. If all credentials referenced by a policy are deleted by this operation, the entire policy is also deleted.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Credentials**.
2. Click the **Search** icon to locate the credentials that you want to view. If you do not specify any additional information, the search includes all credentials in

your domain. To limit the scope of the search, you can search by login ID, description, and resource name. You can also limit your search to checked out credentials by using the **Filter By** option.

3. Select one or more credentials that you want to delete.
4. Click **Delete**.

Checking in credentials

As a privileged administrator, you can check in a credential that was checked out by you or any other user.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Credentials**.
2. Click the **Search** icon to locate the credentials that you want to view. If you do not specify any additional information, the search includes all credentials in your domain. To limit the scope of the search, you can search by login ID, description, and resource name. You can also limit your search to checked out credentials by using the **Filter By** option.
3. Select one or more checked out credentials that you want to check in.
4. Click **Check In**.

Resetting credential password

As a privileged administrator, you can reset the credential password. Resetting the password means changing the credential password and the managed resource password.

Before you begin

Ensure that the credential that you want to reset the password is connected to an identity provider. To connect a credential to an identity provider, see “Connecting a credential to an identity provider.”

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Credentials**.
2. Click the **Search** icon to locate the credentials that you want to view. If you do not specify any additional information, the search includes all credentials in your domain. To limit the scope of the search, you can search by login ID, description, and resource name. You can also limit your search to checked out credentials by using the **Filter By** option.
3. Select one or more connected credentials that you want to reset the password.
4. Click **Reset Password**.

Connecting a credential to an identity provider

As a privileged administrator, you can connect a credential to an identity provider. When you connect a credential to an identity provider, you can share, check in, check out, and reset the password of the credential.

Before you begin

Add a credential that is not connected to an identity provider. See “Adding credentials through Manage Credentials” on page 49.

There must be an account to which you want to connect the credential. The account must meet the following criteria:

- The login ID for the account must be the same as the login ID for the credential.
- The account must be active.

There must be an existing identity provider to which you can connect the credential. See “Adding identity providers” on page 63.

About this task

When you connect a credential to an account, the password for both the credential and the account can be reset by the system so that they are the same. Connecting the credential to an account gives you control over the password on the resource.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Credentials**.
2. Click the **Search** icon to locate the credentials that you want to view. If you do not specify any additional information, the search includes all credentials in your domain. To limit the scope of the search, you can search by login ID, description, and resource name. You can also limit your search to checked out credentials by using the **Filter By** option.
3. Select one or more credentials that you want to connect.

Note: Ensure that there are no credentials with the same login ID. When you connect multiple credentials to a resource, the login ID must be unique.

4. Click **Connect**.
5. On the Select Identity Provider page, select the identity provider from the **Identity provider** list.
6. Review the credentials that you want to connect to the selected identity provider. If you do not want to connect a selected credential, clear the check box next to the login ID. Click **Next**.
7. On the Set Password Options page, complete the following steps:
 - a. Select one of the following password options:

Automatically generate a new password.

Select this option to have the system reset the password for the credential and the account when the system connects them. This option is the preferred option and provides the most security.

Do not change the password.

Select this option if you want the password to remain the same when the credential is connected to the account. If you choose this option, be sure that the passwords for the credential and the account are the same.

- b. The **Change password upon checkin** check box is selected by default. When the check box is selected, the password is changed in the managed resource when the credential is checked in. If you do not want the password to be changed when the credential is checked in, clear the check box. Selecting this check box provides the best security. Once connected, you can change this option under Credential Settings.
- c. In the **Justification** field, provide reasons for connecting the credential to the account.
- d. Click **Connect**.

Disconnecting a credential from an identity provider

As a privileged administrator, you can disconnect a credential from an identity provider. When you disconnect a credential, you can no longer reset the password of the credential since it is not connected to an endpoint anymore.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Credentials**.
2. Click the **Search** icon to locate the credentials that you want to view. If you do not specify any additional information, the search includes all credentials in your domain. To limit the scope of the search, you can search by login ID, description, and resource name. You can also limit your search to checked out credentials by using the **Filter By** option.
3. Select one or more credentials that you want to disconnect from their identity providers.
4. Click **Disconnect**.

What to do next

After the credential is disconnected, you can connect it again to the same identity provider or to another identity provider.

Configuring scheduled password reset

Periodic password rotation is useful for non-exclusive credentials. These are credentials that do not involve check-in and check-out, including those for application identity management scenarios. For these credentials, password changes or resets for every check-in is not a practical option.

About this task

The password reset lifecycle rule specifies how often the rule should check for credentials that are due for a password reset. The password is reset only when the password reset interval for a credential is set and the credential is due for a password reset.

Procedure

1. In service center, click **Manage Credentials**.
2. Ensure that the credential is connected to an identity provider.
3. Select the check box for each credential that you want to change, and click **Edit**.
4. In the **Password Reset Interval** column, specify the number of days.
5. Click **Save**.

What to do next

Configure a lifecycle rule for rotating passwords.

Configuring a lifecycle rule for rotating passwords

You can configure a rule to check for credentials that are due for password resets at specific time intervals.

Procedure

1. In the administrative console, click **Configure System > Manage Life Cycle Rules**.
2. Specify the lifecycle rule level.
3. Click **Add**.
4. Add a lifecycle rule and ensure that the **rotateCredPwd** operation is selected.
5. In the **Event** tab, schedule how often the lifecycle rule is run. For example, you can set the rule to check for credentials that are due for password resets daily every 12 hours.

What to do next

After the lifecycle rotation scheduled run is completed, use the administrative console, and click **View All Requests**. View the **Request Type** for **Rotate Credential Passwords**.

Credential pool management

As a privileged administrator, you can use IBM Security Privileged Identity Manager to manage credential pools. A *credential pool* provides a way to group credentials that have similar access privileges. This grouping can be defined as a *credential tag* or a set of credential tags.

Before working with shared access policies, create an access control item (ACI) for the protection category of **Credential Pool**. See “Default access control items” on page 233.

Creating credential pools

As a privileged administrator, you can create a credential pool.


Before you begin

Ensure that you created an access control item (ACI) for the protection category of **Credential Pool**. For more information about ACIs, see “Access control item management” on page 232.

Procedure

To create a credential pool, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Pool**. The **Select a Pool** page is displayed.
2. Click **Create**. The **Create Pool** wizard is displayed.
3. On the **General Information** page, specify the appropriate values for the pool.
 - a. In the **Pool name** field, type the name of the pool.
 - b. In the **Description** field, type information to explain the purpose of this pool.
 - c. For the **Resource** field, click **Search** to select for a resource for the credential pool.
 - d. On the **Select Resource** page, search for and select a resource and click **OK**. The resource name is displayed in the **Resource** field.
 - e. For the **Business unit** field, click **Search** to select a business unit for the credential pool.

- f. On the Business Unit page, search for and select a business unit and click **OK**. The business unit for that service is displayed in the **Business unit** field.
- g. Optional: To specify roles and users that are associated with this pool, click the twistie icon  next to **Owners**.
 - On the **Role Owners** table:
 - 1) Click **Add** to select role owners for the credential pool.
 - 2) On the Select Roles page, search for and select one or more roles and click **OK**.
 - 3) To remove role owners, select one or more roles and click **Remove**.
 - On the **User Owners** table:
 - 1) Click **Add** to select user owners for the credential pool.
 - 2) On the Select Users page, search for and select one or more users and click **OK**.
 - 3) To remove user owners, select one or more users and click **Remove**.
- h. Click **Next**.
4. On the Rule page, specify the credentials tag as the rule. Type the credential tag that you want to associate with the pool and click **Add**.
5. Optional: To remove credential tags, select one or more tags and click **Delete**.
6. Click **Finish** to create the credential pool.
7. On the Success page, click **Close** to exit.

What to do next

Add credentials to the vault. See “Adding credentials through Manage Credential Vault” on page 37.

Deleting credential pools

As a privileged administrator, you can delete a credential pool. This task deletes only the credential pool. It does not remove the credentials from the vault.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of Credential Pool. For more information about ACIs, see “Access control item management” on page 232.

Procedure

To delete a credential pool, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Pool**. The Select a Pool page is displayed.
2. On the Select a Pool page, click **Search** to locate the credential pool that you want to modify. If you do not specify any additional information, the search includes all credential pools. To limit the scope of the search, complete these steps:
 - a. Optional: In the **Pool name or description** field, specify the name or description associated with the credential pool. For example, type `acmepool` or `pool` for acme company accounts. You can also specify a wildcard, such as `*acme*` to find all pools that contain that term in the name or description.

- b. Optional: Specify a specific resource name in the **Resource name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all resources that contain that term in the name.
- c. Optional: To select a different business unit, click **Search** next to the **Business unit** field.
- d. On the Business Unit page, search for and select a resource and click **OK**. The business unit name is displayed in the **Business unit** field.
- e. Click **Search**. The credential pools that match the search criteria are displayed in the **Credential Pools** table.
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. Select the check box next to one or more credential pools that you want to delete and click **Delete**.
4. On the Confirm page, click **Delete**.
5. On the Success page, click **Close** to exit.

Modifying credential pools

As a privileged administrator, you can modify information about a credential pool. You can change information about the pool, the ownership of the pool, or the group-based rule for the pool.


Before you begin

Ensure that you created an access control item (ACI) for the protection category of `Credential Pool`. For more information about ACIs, see “Access control item management” on page 232.

Procedure

To modify a credential pool, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Pool**. The `Select a Pool` page is displayed.
2. On the `Select a Pool` page, click **Search** to locate the credential pool that you want to modify. If you do not specify any additional information, the search includes all credential pools. To limit the scope of the search, complete these steps:
 - a. Optional: In the **Pool name or description** field, specify the name or description associated with the credential pool. For example, type `acmepool` or `pool` for acme company accounts. You can also specify a wildcard, such as `*acme*` to find all pools that contain that term in the name or description.
 - b. Optional: Specify a specific resource name in the **Resource name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all resources that contain that term in the name.
 - c. Optional: To select a different business unit, click **Search** next to the **Business unit** field. On the Business Unit page, search for and select a service and click **OK**. The business unit name is displayed in the **Business unit** field.
 - d. Click **Search**. The credential pools that match the search criteria are displayed in the **Credential Pools** table.
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. Select the check box next to the credential pool that you want to modify and click **Change**. The Change Pool notebook is displayed.
 4. On the General Information page, specify the values that you want to change for the pool.
 - a. In the **Pool name** field, type the name of the pool.
 - b. Optional: In the **Description** field, type information to explain the purpose of this pool.
 - c. For the **Resource** field, click **Search** to select for a resource for the credential pool.
 - d. On the Select a Resource page, search for and select a resource and click **OK**. The resource name is displayed in the **Resource** field.
 - e. For the **Business unit** field, click **Search** to select a business unit for the credential pool.
 - f. On the Business Unit page, search for and select a service and click **OK**. The business unit for that service is displayed in the **Business unit** field.
 - g. Optional: To specify or change the roles and users that are associated with this pool, click the twistie icon  next to **Owners**.
 - On the **Role Owners** table:
 - 1) Click **Add** to select role owners for the credential pool.
 - 2) On the Select Roles page, search for and select one or more roles and click **OK**.
 - 3) To remove role owners, select one or more roles and click **Remove**.
 - On the **User Owners** table:
 - 1) Click **Add** to select user owners for the credential pool.
 - 2) On the Select Users page, search for and select one or more users and click **OK**.
 - 3) To remove user owners, select one or more users and click **Remove**.
 - h. In the left navigation pane, click **Rule**.
 5. On the Rule page, select the groups that set the group-based rule for the credential pool. Type the name of the group that you want to associate with the pool and click **Add**.
 6. Optional: To remove groups, select one or more groups and click **Delete**.
 7. Click **OK** to save the changes to the credential pool information.
 8. On the Success page, click **Close** to exit.


Viewing credentials in the pool

As a privileged administrator, you can view credentials that are available in the credential pool.

Procedure

To view credentials in the credential pool, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Pool**. The Select a Pool page is displayed.
2. Click **Search** to locate the credentials that you want to modify. If you do not specify any additional information, the search includes all credential pools. To limit the scope of the search, complete these steps:

- a. Optional: In the **Pool name or description** field, specify the name or description associated with the credential pool. For example, type acmepool or pool for acme company accounts. You can also specify a wildcard, such as *acme* to find all pools that contain that term in the name or description.
 - b. Optional: Specify a specific service name in the **Service name** field. For example, type AIX_Service. You can also specify a wildcard, such as *AIX* to find all services that contain that term in the name.
 - c. Optional: To select a different business unit, click **Search** next to the **Business unit** field.
 - d. On the Business Unit page, search for and select a service and click **OK**. The business unit name is displayed in the **Business unit** field.
 - e. Click **Search**. The credential pools that match the search criteria are displayed in the **Credential Pools** table.
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. Locate the row in the **Credential Pools** table that contains the credential pool that you want to view. In the **Name** column, hover your cursor over the  icon to display the action menu. Select **View Credentials in the Pool**.

Note: You do not need to select the check box for the credential in the **Select** column.

The View Credentials in the Pool page is displayed.

4. In the **User ID** field, type the identification name of the credential that you want to view.
5. Optional: Filter the search criteria by using one of the following options:
 - If you want to check in the credentials that are in the vault, select the **Only display credentials in the vault** check box.
 - If you want to check in the credentials that are checked out from the self-service user interface, select the **Only display credentials checked out** check box.

Note: Credentials that are marked with a warning icon are not available in the vault.

6. Click **Search**.

Note: If you leave the **User ID** field blank and click **Search**, all the credentials available in the pool are displayed.

7. Optional: You can also add credentials on the same resource to the pool, or remove credentials from the pool.

Results

The credentials in the pool that meet your search criteria are displayed in the **Credentials In The Pool** table.

Checking in credentials in a credential pool

As a privileged administrator, you can check in a credential that either you or any other user checked out by using the administrative console.

Before you begin

Ensure that you have the following permission: Checking in a credential on behalf of others.

CAUTION:


If the original user still has an active session open while another user has the same shared access account checked out, checking in a shared account for others might break individual accountability. IBM Security Privileged Identity Manager does not make session management on connection to a managed resource. This issue can be addressed by IBM Security Access Manager for Enterprise Single Sign-On integration and automated checkout or checkin.

Procedure

To check in credentials that are checked out, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Manage Credential Pool**. The Select a Pool page is displayed.
2. On the Select a Pool page, click **Search** to locate the credential pool that you want to modify. If you do not specify any additional information, the search includes all credential pools. To limit the scope of the search, complete these steps:
 - a. Optional: In the **Pool name or description** field, specify the name or description associated with the credential pool. For example, type `acmepool` or `pool` for acme company accounts. You can also specify a wildcard, such as `*acme*` to find all pools that contain that term in the name or description.
 - b. Optional: Specify a specific service name in the **Service name** field. For example, type `AIX_Service`. You can also specify a wildcard, such as `*AIX*` to find all services that contain that term in the name.
 - c. Optional: To select a different business unit, click **Search** next to the **Business unit** field.
 - d. On the Business Unit page, search for and select a service and click **OK**. The business unit name is displayed in the **Business unit** field.
 - e. Click **Search**. The credential pools that match the search criteria are displayed in the **Credential Pools** table.

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. Locate the row in the **Credential Pools** table that contains the credential pool that you want to check in. In the **Name** column, hover your cursor over the  icon to display the action menu. Select **View Credentials in the Pool**.

Note: You do not need to select the check box for the credential in the **Select** column.

The View Credentials in the Pool panel is displayed.

4. In the **User ID** field, type the identification name of the credential that you want to check in.
5. Optional: Filter the search criteria by using one of the following options:
 - If you want to check in the credentials that are in the vault, select the **Only display credentials in the vault** check box.

- If you want to check in the credentials that are checked out from the self-service user interface, select the **Only display credentials checked out** check box.

Note: Credentials that are marked with a warning icon are not available in the vault.

6. Click **Search**.

Note: If you leave the **User ID** field blank and click **Search**, all the accounts that are in a group or groups available in the pool are displayed.

7. In the **Credentials In The Pool** table, select one or more credentials that you want to check in.
8. Click **Check In**. A confirmation page is displayed.
9. On the Confirm page, specify the date and time for the checkin to occur, and then click **Check In**, or click **Cancel**. A message is displayed, indicating that you successfully checked in the credential.

Resource management

You can add a resource and associate it to a credential.

A resource refers to an endpoint, host, network device, with a resource alias. An example of a resource is a Linux host. The source has a resource alias, such as a host name or an IP address. On each resource, are privileged credentials such as *root*, that can be managed by IBM Security Privileged Identity Manager.

Adding resources

You can add a resource by specifying the resource name and its endpoint location.

About this task

You can also add resources when you add a credential. See “Adding credentials through Manage Credentials” on page 49.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Resources**.
2. Click **Add**.
3. Provide the following information and click **OK**.

Resource name

Type a name for the resource. This name identifies the repository on which the login ID is hosted. This is used for searching credentials and can be used to link the credential to a policy.

Resource Alias

Optional. Type the IP address or host name of the managed resource to which the credential applies. You can specify multiple resource alias.

Resource Tag

Optional. Enter a resource tag for the managed resource. This tag is used in shared access policies. If your shared access policy entitlement has a matching resource tag, the credential is available at check out. You can specify multiple resource tags.

Results

The added resource is displayed on the Managed Resources page.

Note: The **Credentials** column indicates whether the resource is connected to a credential or not.

What to do next

Add credentials.

Modifying resources

You can update the resource information such as the target host name or IP address.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Resources**.
2. Select the check box next to the resource that you want to edit.
3. Click **Change**.
4. Apply the changes and click **OK**.

Note: You can not modify the Resource UID. You can use this field for shared bulk load operations. See “Shared access bulk load” on page 68.

Deleting resources

You can delete unused resources.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Resources**.
2. Select one or more resources that you want to delete.
3. Click **Delete**.

Identity provider management

Identity providers let you manage passwords of privileged credentials that reside on resources, hosts, or network devices.

To use an identity provider, you add an identity provider entity to establish trust between the managed resource and the identity provider.

The identity provider automates the following tasks:

- Changing credential passwords.
- Validating the existence of the credential's ID on the resource or endpoint.

You can use the identity providers to manage credentials on the following resources:

Table 3. Identity providers for managed resources.

Identity Provider	Description
Active Directory	Requires an agent.
SQL Server	
Windows Local Accounts	
LDAP	Agentless.
POSIX HP-UX	
POSIX AIX®	
POSIX Solaris	
POSIX Linux	
SoftLayer®	
IBM DB2®	

If the identity provider requires an agent, you must install an agent on the managed resource. See the adapter product documentation.

Adding identity providers

Add an identity provider to establish trust with a specific type of managed resource. You can then connect a credential to an identity provider.

Procedure

1. Log on to the Privileged Identity Manager Service Center as a privileged administrator.
2. Click **Manage Identity Providers**.
3. Click **Add**.
4. Specify the options for the type of identity provider that you want to create.

Note: For more information about some of the specific fields, click **Help > Page Help**.

Use the following options as a guide

Service name

Specify a name for the identity provider. For example: F5 Linux

Authentication Mode

Depending on the type of identity provider that you are creating, you can define an identity provider that uses a self-changing password or one that requires authentication that is provided by an administrator.

5. Verify that the identity provider settings are correct.

Modifying identity provider

Modify an existing identity provider to change the authentication details or specify configuration changes.

Procedure

1. Log on to the Privileged Identity Manager Service Center with privileged administrator credentials.
2. Click **Manage Identity Providers**.
3. Select the identity provider and click **Edit**.

Deleting identity providers

You can remove an identity provider that you are no longer using.

Procedure

1. Log on to the Privileged Identity Manager Service Center with privileged administrator credentials.
2. Click **Manage Identity Providers**.
3. Select the identity provider and click **Delete**.

Access administration

Access is the permission to use a set of managed credentials on resources. For example, an access that is called Database administrators might grant its members DBA credentials on all production databases.

Privileged administrators define access in their domains and grant membership to privileged users.

You can use access administration to accomplish the following goals:

- Define sets of credentials that are needed by users who belong to a particular organizational role.
- Grant users membership to access.
- Revoke access rights on resources, if needed.

You can grant access to members with one of the following ways:

By Request

Users can request access to a resource which is then granted according the approval workflow. The access owner can also grant access to members.

By Access Owner

The access owner grants access to users.

By Rule

The users in the admin domain or its subdomains that match an LDAP filter are automatically granted access.

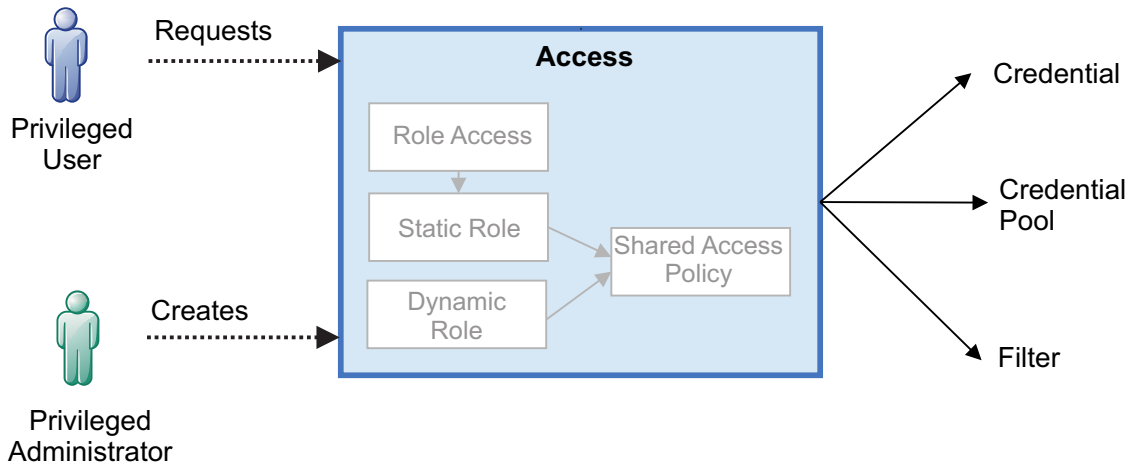


Figure 1. Privileged administrators grant users access to resources with a simplified entitlement model

Access entitlements specify the set of managed credentials or credential pools that members of an access can use.

The entitlement can be defined directly by selecting the credential or credential pool, or dynamically by creating a filter. The filter criteria can include credential or pool name, resource name, and resource tag. When a filter is used, the access will entitle its members to matching credentials that are currently in the vault as well as those that will be added in the future.

Compatibility with earlier versions

Access in IBM Security Privileged Identity Manager Version 2.0.1 subsumes static role, dynamic role, role access, and shared access policy in earlier versions. Shared access entitlements defined in earlier versions of IBM Security Privileged Identity Manager will continue to work.

When an access entitlement is changed using Service Center, the corresponding role is removed from all legacy shared access policies and added to a managed shared access policy.

If a legacy shared access policy has no other roles after this role is removed, it will also be deleted.

Managed shared access policies are listed in the administrative console but cannot be edited directly.

Table 4 shows how access in Service Center maps to roles in the administrative console.

Table 4. Equivalent legacy role for each access assignment type

Access Assignment Type	Legacy role
By owner	Static role without role access
By request	Static role with role access
By rule	Dynamic role

Creating access

As a privileged administrator, you can create access to grant users the permission to use managed credentials.

Before you begin

You are a member of the Privileged Administrator group.

About this task

By default, the **Privileged Administrator View** grants the rights to manage access.

The Privileged Identity Manager administrator or a member of the **System Administrator** group can enable the view for other groups of users.

Procedure

1. In the Privileged Identity Manager Service Center home page, click **Manage Access**.
2. Click **Add**.
3. On the **Access Information** page, provide the following information, and click **Next**.

Access Name

Specify a name that identifies the access on IBM Security Privileged Identity Manager. For example: Database administrators

Description

Optional. Specify information about what the access grants users to, or a remark. For example: Database administrators on production servers.

Assignment Type

Specify how the access is granted.

By Request

Users can request access to a resource, which is then granted according to the approval workflow. The access owner can also grant access to members.

Approval Workflow

Specify the approval process for the access. If no workflow is selected, access requests will be approved directly.

Additional Information

Specify more remarks about the approval process.

By Access Owner

The access owner grants access to users. An access owner is the person who creates the access.

By Rule

The users in the admin domain or subdomains that match an LDAP filter are automatically granted access. You can use the following person attributes in the filter.

Table 5. Person attributes for an LDAP filter

Attribute	Description
cn	Full name.
sn	Last name.
givenname	First name.
initials	Initials.
uid	User ID.
homepostaladdress	Home address.
roomnumber	Office number.
employeenumber	Employee number.
title	Title.
manager	Manager (LDAP Distinguished Name).
postaladdress	Postal address.
secretary	Administrative assistant (LDAP Distinguished Name).
mail	Email address.
telephonenumber	Telephone number.
mobile	Mobile telephone number.
pager	Pager.
homephone	Home telephone number.
eraliases	Aliases.

For example: (&(title=supervisor)(eraliases=engineering))

- On the **Members** page, select the list of members to add, and click **Next**. The **Assignment Type** that you choose in step 3 on page 66, determines the available options on the page.
- On the **Entitlements** page, select the set of privileged credentials, credential pools, or filter a list of credentials that access members are entitled to on the resource.

Credential

Specify entitlements for a set of credentials.

Credential pool

Specify entitlements for a set of credential pools.

Filter Assign entitlements dynamically for credentials or credential pools that meet a set of criteria. All specified criteria must match. The entitlement will include newly added credentials or credential pools that match the filter.

The filter only supports exact match and start with match. For example, enter abc for the exact match of the string, abc* for a string that is starting with abc, abc1, and abc2.

Create a filter for

Define whether the filter applies to credentials or credential pools.

Select all in the current domain

Selects all credentials or credential pools in the current administrative domain.

Entitlement Name

Specify a name for the filter. This field is required.

Login ID

The credential or credential pool name.

Resource Name

The name of the resource that is assigned to the credential or credential pool.

Resource Tag

The tag of the resource that is assigned to the credential or credential pool. A tag is used for grouping resources.

6. Click **Save**.

Changing access

You can change access details such as the access name, members, or entitlements.

Procedure

1. From the Privileged Identity Manager Service Center home page, click **Manage Access**.
2. Select the check box next to the access that you want to change.
3. Click **Change**.
4. On the Change Access page, click each tab and specify the required information for the access.
 - a. On the **Access Information** tab, type information about the access in the field.

Note: You cannot modify the **Assignment Type**.
 - b. On the **Members** tab, specify the members that are granted access. You can add or remove members for access that is granted by an access owner or by a user request. For access that is granted by a rule, you define an LDAP filter.
 - c. On the **Entitlements** tab, specify the entitlements to a set of credentials or credential pools that members can access. You create an entitlement by selecting a set of credentials or credential pools. You can also use a filter. After selecting the entitlement type and credentials, click **Add**.
5. When your changes are done, click **Submit**.

Shared access bulk load

As a privileged administrator, you can add credentials or credential pools to the vault using shared access bulk load. You can also modify information for the credentials or credential pools that are in the credential vault. IBM Security Privileged Identity Manager uses the settings that are indicated in a CSV file to add or update the credentials or credential pools.

Shared access bulk load operations

As a privileged administrator, you can use a comma-separated value (CSV) file to complete credential and credential pool-related operations in bulk.

A shared access CSV file supports the following operations:

- Adding credentials (whether connected to an account or not connected to an account) in bulk to the credential vault.

- Modifying existing credential settings in bulk
- Modifying existing credential passwords that are stored in the credential vault in bulk
- Creating credential pools in bulk
- Modifying existing credential pool settings in bulk
- Connecting credentials to identity providers in bulk
- Disconnecting credentials from identity providers in bulk

Format of the shared access CSV file

A shared access comma-separated value (CSV) file might consist of multiple sections, each of which contains three elements.

Each section of the CSV file contains the following three elements:

Type identifiers

The first line in the file is a *type identifier* that identifies the entity type. For example, the type identifier of a shared access CSV file can be `#Credentials_v2`, `#CredentialPools_v2`, `#CredentialPools`, or `#Credentials`.

Note: The `#Credentials` and `#CredentialPool` type identifiers are deprecated and is provided for users with existing CSV files from a previous release. If you use this type identifier, read the column header descriptions because some of them have changed. It is suggested, however, that you use the `#Credentials_v2` and `#CredentialPools_v2` type identifiers instead of the `#Credentials` and `#CredentialPools` type identifiers in your CSV files.

Column headers

A type identifier is followed by column headers. Column headers are attribute names that represent columns in a CSV file. Column headers are separated by commas in the CSV file.

Note: Column headers for the `#Credentials_v2`, `#CredentialPools`, and `#Credentials` type identifiers are different. For information about the column headers, see the following topics:

- “The `#Credentials_v2` type identifier column headers”
- “The `#CredentialPools` type identifier column headers” on page 73
- “The `#Credentials` type identifier column headers” on page 82
- “The `#CredentialPools_v2` type identifier column headers” on page 78

Actual data

A column header is followed by actual data that includes details of each attribute in that section.

Note: Some attributes are required and others are optional in the CSV file. For optional attributes, you can specify only the columns and attributes that are important to you and for which the value is different from the default.

The `#Credentials_v2` type identifier column headers

A shared access comma-separated value (CSV) file can include `#Credentials_v2` type identifier column headers. It is suggested that you use the `#Credentials_v2` type identifier instead of the `#Credentials` type identifier in your CSV files. The `#Credentials` type identifier is deprecated and is provided for users with existing CSV files from a previous release.

The following list describes the #Credentials_v2 type identifier column headers that you can use in the CSV file.

ACCOUNT_UID

Required. Specifies the user ID that is associated with the credential.

ORG_URI

Specifies the organizational container under which the credential must be created. The organizational container might be an admin domain, organizational unit, or location, for example. However, if the ORG_URI value is not specified but the ORG_PDN value is provided, then IBM Security Privileged Identity Manager uses the ORG_PDN attribute value. If neither of the attributes is provided or if the ORG_URI or ORG_PDN value is incorrect, then the entry is invalid.

This attribute specifies the Uniform Resource Identifier. You can add this field by adding the `eruri` attribute to the container form template when you design forms.

You must specify either ORG_URI or ORG_PDN when you create a credential. Specifying these attributes is optional when you update the credential.

ORG_PDN

Specifies the container DN that uniquely identifies:

- An organizational container.
- An organization pseudo DN (ORG_PDN) that might be associated with one or more organizational containers.

An organization pseudo DN can be associated with multiple organizational containers. In this case, IBM Security Privileged Identity Manager considers the first organizational container as the container under which the credential must be created.

The following pseudo BNF notation represents the syntax for ORG_PDN:

```
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
```

For example:

```
l=San Francisco,ou=Admin,o=ibm
```

You must specify either ORG_URI or ORG_PDN when you create a credential. Specifying these attributes is optional when you update the credential.

RESET_PASSWORD

Optional. Specifies whether the password must be reset after adding the credential to the vault. The valid values are TRUE and FALSE. The default value is FALSE.

PASSWORD

Optional. Specifies the password of the credential. If the credential already exists and the specified password is different from the password that is stored in the vault, the credential password in the vault will be updated.

DESCRIPTION

Optional. Provides a brief description about the credential that is added to the credential vault.

USE_DEFAULT_SETTINGS

Optional. Specifies whether to apply the global default settings to the

credentials. The valid values are TRUE and FALSE. If this setting is TRUE, then the other credential settings columns are ignored.

Note: If this column is not specified, the value is set as follows:

- If none of the credential setting columns (ACCESS_MODE, PASSWORD_VIEWABLE, MAX_CHECKOUT_DURATION, ENABLE_CHECKOUT_SEARCH, RESET_PASSWORD_ON_CHECKIN) are specified, the USE_DEFAULT_SETTINGS value is set to TRUE.
- If at least one of the credential setting columns is specified, the credential will not use global default settings; the USE_DEFAULT_SETTINGS value is set to FALSE.

ACCESS_MODE

Optional. Specifies the access mode of the credentials. You can use the following valid values:

- 0 indicates exclusive permissions. (Requires checkout and checkin.)
- 1 indicates nonexclusive permissions. (Does not require checkout and checkin.)
- 2 indicates nonshared credentials. (Credential is not shared.)

If you do not specify a value, then the default value is 0 (exclusive).

PASSWORD_VIEWABLE

Optional. Specifies whether to display the credential password to users on the self-service user interface. The default value is TRUE.

MAX_CHECKOUT_DURATION

Optional. Specifies how long a credential can be checked out. Specify the time in weeks, days, or hours by adding the suffix, as described in the following examples:

- 8 w indicates eight weeks.
- 8 d indicates eight days.
- 8 h indicates eight hours.

If you do not specify a value, then the default time duration is 8 h.

ENABLE_CHECKOUT_SEARCH

Optional. Specifies whether the checkout search is enabled for the credential on the self-service user interface. The default value is TRUE, which indicates that the checkout search is enabled for the credentials on the self-service user interface. To disable the checkout search for credentials, specify FALSE.

RESET_PASSWORD_ON_CHECKIN

Optional. Specifies whether the password must be reset on the self-service user interface after you check in a credential. You must specify this attribute if the access mode value is 0. The default value is TRUE, which indicates that the password is reset on the self-service user interface after you check in a credential. If you do not want the password to be reset after you check in a credential, specify FALSE. This value is valid only for a credential that you are connecting to an account.

RESOURCE_UID

Uniquely identifies the resource for which you are adding credentials to the vault. Identifies the repository on which this user ID is hosted. For example, the unique identifier might be the IP address or the URL of a host or application. _UID is required if CONNECT_SERVICE_PDN is not specified. You must specify at least one of these two columns.

NEW_RESOURCE_UID

Optional. Specifies the new value for the resource UID. Specify this setting only if you want to modify the credential service UID for an existing credential. If the credential does not exist, this setting is ignored.

RESOURCE_NAME

Optional. Specifies a common name for the resource for which you are adding credentials to the vault. This common name identifies the repository on which this user ID is hosted. For example, the name might be Department UNIX system.

If this setting is not specified, it is set to the value of the `_UID`.

RESOURCE_ALIAS

Optional. Used if you also use IBM Security Access Manager for Enterprise Single Sign-On. IBM Security Access Manager for Enterprise Single Sign-On uses the service alias, along with the credential name, to find the credential in IBM Security Identity Manager. This field must match the **ISIM Authentication Service ID** (for example, `pim_auth_service`) that is defined when mapping the authentication service.

You can specify multiple service aliases, separated by vertical bar (|) characters; for example,
`service_alias_1|service_alias_2|service_alias_3`.

RESOURCE_TAG

Optional. If you have a shared access policy that specifies a particular service tag, and you want the policy to work for the credential, specify the service tag in this field.

You can specify multiple service tags, separated by vertical bar (|) characters; for example, `service_tag_1|service_tag_2|service_tag_3`.

CONNECT_SERVICE_PDN

Required only when you are adding a credential from an account or connecting a credential to an account. Specifies the service distinguished name (DN) that uniquely identifies a service or a service pseudo DN for the account to which you are connecting the credential. If multiple accounts are found for the `CONNECT_SERVICE_PDN` specified, or if no accounts are found for it, this entry will fail, and an error message is logged. If you specify a blank value for this column, the resource aliases are cleared.

The following pseudo Backus-Naur Form (BNF) notation represents the syntax for `CONNECT_SERVICE_PDN`:

```
servicePDN ::= serviceAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
serviceAttr ::= string (Must be a valid attribute name of the service.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
description=winlocalService,l=San Francisco,ou=Admin,o=ibm
```

DISCONNECT

Optional. Specifies whether to disconnect the credential from the account. Specify `TRUE` if you want to disconnect the credential from the account or `FALSE` if you do not want to disconnect.

When a credential is disconnected from the associated account:

- Users can still check out the credential, but the system cannot reset the password when the credential is checked back in.
- The account password is not synchronized to the credential vault when the account password is changed.

CREDENTIAL_TAG

Optional. Specifies the credential tags. You can specify multiple tags in the following format: tag1|tag2|tag3

This attribute is used to group credentials into a pool. If the credential tags match the rule definition of a pool that resides on the same resource, the credential is resolved as a member of the pool.

First example

The following sample CSV file contains information about the credentials to be added or updated in the credential vault:

```
#Credentials_v2
ACCOUNT_UID,ORG_PDN,PASSWORD,RESOURCE_UID,RESOURCE_NAME
vicgreen,"ou=Finance,o=Organization",not_secret,vic.samplecompany.com,Vic's Linux Service
```

In this example, the credential (user ID vicgreen, password not_secret) is added to the credential vault. The _UID is a URL, vic.samplecompany.com. Global credential settings are used. Other than the password and the resource name, only the required attributes are specified.

The shared access CSV file lists the column headers in a default sequence. You can change the sequence of these column headers according to your requirements. However, do not change the name of these column headers.

Second example

```
#Credentials_v2
ACCOUNT_UID,RESOURCE_UID,RESOURCE_NAME,ORG_PDN,PASSWORD_VIEWABLE
vicgreen,vic.samplecompany.com,Vic's Linux Service,"ou=Finance,o=Organization",false
```

In this example, the user specifies only required fields and the fields that are important and do not match the defaults. The credential (user ID vicgreen, password not_secret) is added to the vault. The password is not viewable, and the other credential settings use the defaults. That is, the access mode is exclusive (checkout is required), the maximum checkout duration is 8 hours, and checkout search is enabled.

Third example

```
#Credentials_v2
ACCOUNT_UID,ORG_PDN,PASSWORD,RESOURCE_UID,RESOURCE_NAME,
CONNECT_SERVICE_PDN
vicgreen,"ou=Finance,o=Organization",not_secret,vic.samplecompany.com,
Vic's Linux Service,Vic_Linux|VicGreen_Linux,description=winlocalService,
l=San Francisco,ou=Admin,o=ibm
```

Note: Be sure to specify all of the data on one line in your CSV file. The data is divided into two lines in the example for display purposes.

In this example, credential vicgreen is added from the winlocal account.

The #CredentialPools type identifier column headers

This section lists the #CredentialPools type identifier column headers in a shared access comma-separated value (CSV) file.

POOL_PDN

Specifies the credential pool distinguished name (DN) that uniquely identifies a credential pool or a credential pool pseudo DN (POOL_PDN). A credential pool pseudo DN might be associated with multiple credential pools. In this case, IBM Security Privileged Identity Manager attempts to update all the pools with the specified values in the CSV file for description, owners, or groups. This attribute is optional; however, you must specify this attribute to update an existing credential pool.

The following pseudo Backus-Naur Form (BNF) notation represents the syntax for POOL_PDN:

```
PoolPDN ::= poolAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
poolAttr ::= string (Must be a valid attribute name of the credential pool.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
description=winlocalService,l=San Francisco,ou=Admin,o=ibm
```

IBM Security Privileged Identity Manager initially resolves to ORG_PDN to resolve to the POOL_PDN. The ORG_PDN is resolved to one or more organizational containers. In the previous example, IBM Security Privileged Identity Manager resolves to the specified ORG_DN (l=San Francisco,ou=Admin,o=ibm) in a particular manner; that is, IBM Security Privileged Identity Manager searches for the location San Francisco that is located under the organizational unit Admin under the organization ibm. From all the organizational containers that are obtained, IBM Security Privileged Identity Manager then searches for the credential pools under the specified criteria; that is, it searches for all the credential pools that have a description of winlocalService.

POOL_NAME

Specifies the name of a credential pool. If you do not specify this attribute, IBM Security Privileged Identity Manager generates a name in the *\$service name-\$group name* format. This attribute is optional.

SERVICE_URI

Specifies the URI that uniquely identifies the service. This attribute is required when you create a credential pool or optional when you update the credential pool.

SERVICE_PDN

Specifies the service distinguished name (DN) that uniquely identifies a service or a service pseudo DN (SERVICE_PDN). A service pseudo DN might be associated with multiple services. If the service pseudo DN is associated with multiple services, IBM Security Privileged Identity Manager creates a pool under each of those associated services. All these services must have a minimum of one group specified in the CSV file. If a service does not have a group specified, IBM Security Privileged Identity Manager does not use that service to create the pool. If none of the services has the specified group or groups, then the entry is invalid. This attribute is required when you create a credential pool and optional when you update the credential pool.

Note: IBM Security Privileged Identity Manager uses the SERVICE_URI attribute value to resolve or identify the service. If the SERVICE_URI value is

not specified but the SERVICE_PDN is provided, then IBM Security Privileged Identity Manager uses the SERVICE_PDN attribute value. If the SERVICE_URI attribute value is incorrect, then the entry is invalid.

GROUP_UID

Lists the groups that comprise the credential pool. You can specify multiple groups in the following format:

```
grp1|grp2|grp3
```

This attribute is required only when you create a credential pool. Ensure that you specify all the groups that belong to the same specified service.

Note: When you update an existing credential pool for which the GROUP_UID is specified, IBM Security Privileged Identity Manager replaces existing groups in the credential pool.

PERSON_URI

Specifies the user owner of the credential pool. IBM Security Privileged Identity Manager uses the PERSON_URI attribute value as the owner of the credential pool. If the PERSON_URI value is not specified but the PERSON_PDN is provided, then IBM Security Privileged Identity Manager uses the PERSON_PDN attribute value. If the PERSON_URI value is specified and it does not resolve to any person, then IBM Security Privileged Identity Manager displays a warning message. This attribute is optional.

PERSON_PDN

Specifies the person distinguished name (DN) that uniquely identifies a person or a person pseudo DN (PERSON_PDN). A person pseudo DN might be associated with multiple persons. If the person pseudo DN is associated with multiple persons, IBM Security Privileged Identity Manager associates all of them as the owner of the credential pool. All of these associated persons must be under the same base organization as a service. If none of the persons is from the same base organization, IBM Security Privileged Identity Manager:

- Ignores this attribute value.
- Logs a warning message in the trace.log file.

The following pseudo BNF notation represents the syntax for PERSON_PDN:

```
PersonPDN ::= poolAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
personAttr ::= string (Must be a valid attribute name of the person.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
cn=John,l=San Francisco,ou=Admin,o=ibm
```

IBM Security Privileged Identity Manager initially resolves to ORG_PDN to resolve to the PERSON_PDN. The ORG_PDN is resolved to one or more organizational containers. In the previous example, IBM Security Privileged Identity Manager resolves to the specified ORG_DN (l=San Francisco,ou=Admin,o=ibm) in a particular manner; that is, IBM Security Privileged Identity Manager searches for the location San Francisco that is located under the organizational unit Admin under the organization ibm. From all the organizational containers that are obtained, IBM Security

Privileged Identity Manager then searches for the person under the specified criteria; that is, it searches for all the persons that have the name as John and return the first occurrence of such a person. This attribute is optional.

You can specify multiple values for this attribute, which can contain personDN and personPDN. For example:

```
personDN1|personPDN2|personDN2
```

ROLE_URI

Specifies the role owner of the credential pool. IBM Security Privileged Identity Manager uses the ROLE_URI attribute value as the owner of the credential pool. If the ROLE_URI value is not specified but the ROLE_PDN value is specified, then IBM Security Privileged Identity Manager uses the ROLE_PDN attribute value. If the ROLE_URI value is specified and it does not associate with any role, then IBM Security Privileged Identity Manager displays a warning message. This attribute is optional.

ROLE_PDN

Specifies the person distinguished name (DN) that uniquely identifies a role or a role pseudo DN (ROLE_PDN). A role pseudo DN might be associated with multiple roles. If the role pseudo DN is associated with multiple roles, IBM Security Privileged Identity Manager associates all of them as the owner of the credential pool. All of these associated roles must be under the same base organization as a service. This attribute is optional.

If none of the roles is from the same base organization, IBM Security Privileged Identity Manager:

- Ignores this attribute value.
- Logs a warning message in the trace.log file.

The following pseudo BNF notation represents the syntax for ROLE_PDN:

```
rolePDN ::= roleAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
roleAttr ::= string (Must be a valid attribute name of the role.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
description=admin,l=San Francisco,ou=Admin,o=ibm
```

You can specify multiple values for this attribute, which can contain roleDN and rolePDN. For example:

```
roleDN1|rolePDN2|roleDN2
```

ORG_URI

Specifies the organizational container under which the credential pool must be created. The organizational container might be an organization, organizational unit, location, and so on. IBM Security Privileged Identity Manager uses the ORG_URI attribute value as the organizational container under which the credential pool must be created. However, if the ORG_URI value is not specified but the ORG_PDN value is provided, then IBM Security Privileged Identity Manager uses the ORG_PDN attribute value. If neither of the attributes is provided or if the ORG_URI or ORG_PDN value is incorrect, then the entry is invalid. You must specify either ORG_URI or ORG_PDN when you create a credential pool. Specifying these attributes is optional when you update the credential pool.

ORG_PDN

Specifies the container DN that uniquely identifies:

- An organizational container.
- An organization pseudo DN (ORG_PDN) that might be associated with one or more organizational containers.

An organization pseudo DN can be associated with multiple organizational containers. In this case, IBM Security Privileged Identity Manager considers the first organizational container as the container under which the credential pool must be created.

The following pseudo BNF notation represents the syntax for ORG_PDN:

```
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
orgAttr ::= string (Must be a valid attribute name of the organizational
container.)
```

For example:

```
l=San Francisco,ou=Admin,o=ibm
```

You must specify either ORG_URI or ORG_PDN when you create a credential pool. Specifying these attributes is optional when you update the credential pool.

DESCRIPTION

Provides a brief description about the credential pool that must be added to the credential vault. This attribute is optional.

Sample CSV file for adding information to or updating credential pools

The following sample CSV file contains information about the credential pools that must be added or updated:

```
#CredentialPools
POOL_PDN,POOL_NAME,SERVICE_URI,SERVICE_PDN,GROUP_UID,PERSON_URI,PERSON_PDN,
ROLE_URI,ROLE_PDN,ORG_URI,ORG_PDN,DESCRIPTION
,ITIMPool,, "erglobalid=00000000000000000002,
ou=services,erglobalid=000000000000000000,ou=org,dc=com",Manager,Both,,
"erglobalid=2508992138323996132,ou=0,ou=people,erglobalid=000000000000000000,ou=org,dc=com",,
"erglobalid=00000000000000000001,ou=roles,erglobalid=000000000000000000,
ou=org,dc=com|erglobalid=2535139933528048671,ou=roles,erglobalid=000000000000000000,
ou=org,
dc=com",, "erglobalid=2508777664488232255,ou=orgChart,erglobalid=000000000000000000,ou=org,dc=com",
"ITIM Pool Description"
```

Sample CSV file for adding information to the credential pool

The following sample CSV file contains information to add to the credential pool:

```
#CredentialPools
POOL_PDN,POOL_NAME,SERVICE_URI,SERVICE_PDN,GROUP_UID,PERSON_URI,
PERSON_PDN,ROLE_URI,ROLE_PDN,ORG_URI,ORG_PDN,DESCRIPTION
,IBMBufferPool,, "description=test,l=Pune,ou=Finance,o=Organization","Users|Guests",,,,
"description=test,o=Organization",,"o=Organization",testpool
```

Sample CSV file for modifying the credential pool

The following sample CSV file contains information to modify the existing credential pool:

```
#CredentialPools
POOL_PDN,POOL_NAME,SERVICE_URI,SERVICE_PDN,GROUP_UID,PERSON_URI,PERSON_PDN,ROLE_URI,
ROLE_PDN,ORG_URI,ORG_PDN,DESCRIPTION
"description=testpool,l=Pune,ou=Finance,o=Organization",IBMBufferPool,,,"Guests|Helpdesk",,,,
"description=test,o=Organization",,"o=Organization",test_desc
```

Note: When you modify an existing credential pool, the POOL_PDN attribute is mandatory.

The #CredentialPools_v2 type identifier column headers

This section lists the #CredentialPools_v2 type identifier column headers in a shared access comma-separated value (CSV) file.

POOL_PDN

Specifies the credential pool distinguished name (DN) that uniquely identifies a credential pool or a credential pool pseudo DN (POOL_PDN). A credential pool pseudo DN might be associated with multiple credential pools. In this case, IBM Security Privileged Identity Manager attempts to update all the pools with the specified values in the CSV file for description, owners, or groups. This attribute is optional; however, you must specify this attribute to update an existing credential pool.

The following pseudo Backus-Naur Form (BNF) notation represents the syntax for POOL_PDN:

```
PoolPDN ::= poolAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
poolAttr ::= string (Must be a valid attribute name of the credential pool.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
description=winlocalService,l=San Francisco,ou=Admin,o=ibm
```

IBM Security Privileged Identity Manager initially resolves to ORG_PDN to resolve to the POOL_PDN. The ORG_PDN is resolved to one or more organizational containers. In the previous example, IBM Security Privileged Identity Manager resolves to the specified ORG_DN (l=San Francisco,ou=Admin,o=ibm) in a particular manner; that is, IBM Security Privileged Identity Manager searches for the location San Francisco that is located under the organizational unit Admin under the organization ibm. From all the organizational containers that are obtained, IBM Security Privileged Identity Manager then searches for the credential pools under the specified criteria; that is, it searches for all the credential pools that have a description of winlocalService.

POOL_NAME

Specifies the name of a credential pool. If you do not specify this attribute, IBM Security Privileged Identity Manager generates a name in the *\$service name-\$group name* format. This attribute is optional.

RESOURCE_UID

Uniquely identifies the resource for which you are adding the credential pool to the vault. Identifies the repository on which the pool members are hosted. For example, the unique identifier might be the IP address or the URL of a host or application. RESOURCE_UID is required if POOL_PDN is not specified. You must specify at least one of these two columns.

POOL_RULE

Lists the credential tags that comprise the credential pool. Only credentials on the same resource and tagged with these values are resolved as the pool members. You can specify multiple tags in the following format:
tag1|tag2|tag3

This attribute is required only when you create a credential pool.

Note: When you update an existing credential pool for which the `POOL_RULE` is specified, IBM Security Privileged Identity Manager replaces existing rule in the credential pool.

PERSON_URI

Specifies the user owner of the credential pool. IBM Security Privileged Identity Manager uses the `PERSON_URI` attribute value as the owner of the credential pool. If the `PERSON_URI` value is not specified but the `PERSON_PDN` is provided, then IBM Security Privileged Identity Manager uses the `PERSON_PDN` attribute value. If the `PERSON_URI` value is specified and it does not resolve to any person, then IBM Security Privileged Identity Manager displays a warning message. This attribute is optional.

PERSON_PDN

Specifies the person distinguished name (DN) that uniquely identifies a person or a person pseudo DN (`PERSON_PDN`). A person pseudo DN might be associated with multiple persons. If the person pseudo DN is associated with multiple persons, IBM Security Privileged Identity Manager associates all of them as the owner of the credential pool. All of these associated persons must be under the same base organization as a service. If none of the persons is from the same base organization, IBM Security Privileged Identity Manager:

- Ignores this attribute value.
- Logs a warning message in the `trace.log` file.

The following pseudo BNF notation represents the syntax for `PERSON_PDN`:

```
PersonPDN ::= poolAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
personAttr ::= string (Must be a valid attribute name of the person.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
cn=John,l=San Francisco,ou=Admin,o=ibm
```

IBM Security Privileged Identity Manager initially resolves to `ORG_PDN` to resolve to the `PERSON_PDN`. The `ORG_PDN` is resolved to one or more organizational containers. In the previous example, IBM Security Privileged Identity Manager resolves to the specified `ORG_DN` (`l=San Francisco,ou=Admin,o=ibm`) in a particular manner; that is, IBM Security Privileged Identity Manager searches for the location San Francisco that is located under the organizational unit Admin under the organization ibm. From all the organizational containers that are obtained, IBM Security Privileged Identity Manager then searches for the person under the specified criteria; that is, it searches for all the persons that have the name as John and return the first occurrence of such a person. This attribute is optional.

You can specify multiple values for this attribute, which can contain personDN and personPDN. For example:

```
personDN1|personPDN2|personDN2
```

ROLE_URI

Specifies the role owner of the credential pool. IBM Security Privileged Identity Manager uses the ROLE_URI attribute value as the owner of the credential pool. If the ROLE_URI value is not specified but the ROLE_PDN value is specified, then IBM Security Privileged Identity Manager uses the ROLE_PDN attribute value. If the ROLE_URI value is specified and it does not associate with any role, then IBM Security Privileged Identity Manager displays a warning message. This attribute is optional.

ROLE_PDN

Specifies the person distinguished name (DN) that uniquely identifies a role or a role pseudo DN (ROLE_PDN). A role pseudo DN might be associated with multiple roles. If the role pseudo DN is associated with multiple roles, IBM Security Privileged Identity Manager associates all of them as the owner of the credential pool. All of these associated roles must be under the same base organization as a service. This attribute is optional.

If none of the roles is from the same base organization, IBM Security Privileged Identity Manager:

- Ignores this attribute value.
- Logs a warning message in the trace.log file.

The following pseudo BNF notation represents the syntax for ROLE_PDN:

```
RolePDN ::= roleAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
roleAttr ::= string (Must be a valid attribute name of the role.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
description=admin,l=San Francisco,ou=Admin,o=ibm
```

You can specify multiple values for this attribute, which can contain roleDN and rolePDN. For example:

```
roleDN1|rolePDN2|roleDN2
```

ORG_URI

Specifies the organizational container under which the credential pool must be created. The organizational container might be an organization, organizational unit, location, and so on. IBM Security Privileged Identity Manager uses the ORG_URI attribute value as the organizational container under which the credential pool must be created. However, if the ORG_URI value is not specified but the ORG_PDN value is provided, then IBM Security Privileged Identity Manager uses the ORG_PDN attribute value. If neither of the attributes is provided or if the ORG_URI or ORG_PDN value is incorrect, then the entry is invalid. You must specify either ORG_URI or ORG_PDN when you create a credential pool. Specifying these attributes is optional when you update the credential pool.

ORG_PDN

Specifies the container DN that uniquely identifies:

- An organizational container.

Note: When you modify an existing credential pool, the POOL_PDN attribute is mandatory.

The #Credentials type identifier column headers

A shared access comma-separated value (CSV) file can include #Credentials type identifier column headers. The #Credentials type identifier is deprecated and is provided for users with existing CSV files from a previous release. If you use this type identifier, read the column header descriptions because some of them have changed. It is suggested, however, that you use the #Credentials_v2 type identifier instead of the #Credentials type identifier in your CSV files.

Note:

Two column headers, ORG_URI and ORG_PDN, are added for this release.

In previous releases, the USE_DEFAULT_SETTINGS column header is called USE_GLOBAL_SETTINGS.

The following list describes the columns that you can define in the CSV file.

ORG_URI

Optional. Specifies the organizational container under which the credential must be created. The organizational container might be an admin domain, organizational unit, or location, for example. However, if the ORG_URI value is not specified but the ORG_PDN value is provided, then IBM Security Privileged Identity Manager uses the ORG_PDN attribute value. If the ORG_URI or ORG_PDN value is incorrect, then the entry is invalid.

This attribute specifies the Uniform Resource Identifier. You can add this field by adding the eruri attribute to the container form template when you design forms.

ORG_PDN

Optional. Specifies the container DN that uniquely identifies:

- An organizational container.
- An organization pseudo DN (ORG_PDN) that might be associated with one or more organizational containers.

An organization pseudo DN can be associated with multiple organizational containers. In this case, IBM Security Privileged Identity Manager considers the first organizational container as the container under which the credential must be created.

The following pseudo BNF notation represents the syntax for ORG_PDN:

```
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
```

For example:

```
l=San Francisco,ou=Admin,o=ibm
```

SERVICE_URI

Specifies the URI that uniquely identifies the service.

You must specify this attribute if SERVICE_PDN, SERVICE_ORG_CONT_URI, or SERVICE_ORG_CONT_PDN is not specified.

SERVICE_PDN

Specifies the service distinguished name (DN) that uniquely identifies a service or a service pseudo DN (SERVICE_PDN). A service pseudo DN might

be associated with multiple services. If the service pseudo DN is associated with multiple services, IBM Security Privileged Identity Manager adds the credential to the credential vault for all those services. You can specify the SERVICE_TYPE attribute to filter the services. If none of the identified services has the specified ACCOUNT_UID, then that credential entry is invalid.

You must specify this attribute if either SERVICE_URI, SERVICE_ORG_CONT_URI, or SERVICE_ORG_CONT_PDN is not specified.

The following pseudo Backus-Naur Form (BNF) notation represents the syntax for SERVICE_PDN:

```
servicePDN ::= serviceAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
serviceAttr ::= string (Must be a valid attribute name of the service.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
description=winlocalService,l=San Francisco,ou=Admin,o=ibm
```

IBM Security Privileged Identity Manager initially resolves to ORG_PDN to resolve to the SERVICE_PDN. The ORG_PDN is resolved to one or more organizational containers. In the previous example, IBM Security Privileged Identity Manager resolves to the specified ORG_DN (l=San Francisco,ou=Admin,o=ibm) in a particular manner. That is, IBM Security Privileged Identity Manager searches for the location San Francisco that is located inside the organizational unit Admin under the organization ibm. From all the organizational containers that are obtained, IBM Security Privileged Identity Manager then searches for the services under the specified criteria. That is, it searches for all the services that have description as winlocalService.

SERVICE_ORG_CONT_URI

Specifies the URI that uniquely identifies the organizational container, such as admin domain, organizational unit, and location. All the services under the organizational container that match the specified SERVICE_TYPE attribute value might be considered to process the entry. IBM Security Privileged Identity Manager attempts to add the credentials for the account that is identified by the ACCOUNT_UID to the credential vault for all those services. If none of the identified services has the specified ACCOUNT_UID, then that credential entry is invalid.

You must specify this attribute if either SERVICE_URI, SERVICE_PDN, or SERVICE_ORG_CONT_PDN is not specified.

SERVICE_ORG_CONT_PDN

Specifies one of the following details:

- An OrgDN that uniquely identifies the organizational container, such as organization, organizational unit, and location.
- An organization pseudo DN that might be associated with one or more organizational containers.

An attribute might specify one or more organizational containers. In this case, IBM Security Privileged Identity Manager uses all the services under each organizational container that match the specified SERVICE_TYPE attribute to process the entry. IBM Security Privileged Identity Manager adds the credentials for the account that is identified by the ACCOUNT_UID to the credential vault for all those services that match the SERVICE_TYPE

attribute value. If none of the identified services has the specified ACCOUNT_UID, then that credential entry is invalid

You must specify this attribute if SERVICE_URI, SERVICE_PDN, or SERVICE_ORG_CONT_URI is not specified.

The following pseudo BNF notation represents the syntax for SERVICE_ORG_CONT_PDN:

```
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
```

For example:

```
l=San Francisco,ou=Admin,o=ibm
```

IBM Security Privileged Identity Manager initially resolves to ORG_PDN to resolve to the SERVICE_PDN. The ORG_PDN is resolved to one or more organizational containers. In the previous example, IBM Security Privileged Identity Manager resolves to the specified ORG_DN (l=San Francisco,ou=Admin,o=ibm) in a particular manner. That is, IBM Security Privileged Identity Manager searches for the location San Francisco that is located inside the organizational unit Admin under the organization ibm.

Note: IBM Security Privileged Identity Manager uses SERVICE_URI, SERVICE_PDN, SERVICE_ORG_CONT_URI, and SERVICE_ORG_CONT_PDN to resolve one or more services to process the entry. However, only one attribute value is considered for a single entry. IBM Security Privileged Identity Manager uses the attribute value from left to right. The SERVICE_URI attribute value is considered first. If SERVICE_URI is not specified, SERVICE_PDN is considered. If an attribute value does not resolve to a service, then that credential entry is invalid.

SERVICE_TYPE

Specifies the type of service.

You must specify this attribute if you specified SERVICE_ORG_CONT_URI or SERVICE_ORG_CONT_PDN.

The following service type names are provided with the IBM Security Privileged Identity Manager product. However, the system administrator can add others.

- LdapProfile
- PosixAixProfile
- PosixHpuxProfile
- PosixLinuxProfile
- PosixSolarisProfile

ACCOUNT_UID

Required. Specifies the account ID.

DESCRIPTION

Optional. Provides a brief description about the credential that must be added to the credential vault.

OWNER_URI

Identifies the unique owner of the account. The owner attributes are optional. However, if the account is an orphan account, then the owner attributes are required.

Note: Either the OWNER_URI or the OWNER_PDN must be specified.

OWNER_PDN

Specifies a person DN that uniquely identifies a person or a person pseudo DN (personPDN). A person pseudo DN can be associated with multiple persons. IBM Security Privileged Identity Manager considers the first person in the list as the owner. If the account is an orphan account, IBM Security Privileged Identity Manager uses the owner to adopt the account. However, if the account is not an orphan account, specifying an owner (OWNER_URI or OWNER_PDN) transfers the account to the new owner.

The following pseudo BNF notation represents the syntax for OWNER_PDN:

```
personPDN ::= personAttr '=' value ',' orgDn
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= orgAttr '=' value
personAttr ::= string (Must be a valid attribute name of the person.)
orgAttr ::= string (Must be a valid attribute name of the organizational container.)
value ::= string
```

For example:

```
cn=James,l=San Francisco,ou=Admin,o=ibm
```

IBM Security Privileged Identity Manager initially resolves to ORG_PDN before resolving to the OWNER_PDN. The ORG_PDN is resolved to one or more organizational containers. Therefore, in the previous example, IBM Security Privileged Identity Manager resolves to the specified ORG_DN (l=San Francisco,ou=Admin,o=ibm) in a particular manner. That is, IBM Security Privileged Identity Manager searches for the location San Francisco that is located inside the organizational unit Admin under the organization ibm. From all the organizational containers that are retrieved, IBM Security Privileged Identity Manager searches for the person with the specified criteria. That is, it searches for all the persons with the name James and returns the first occurrence of such a person.

OWNERSHIP_TYPE

Required if the owner is specified. Identifies the ownership type of the account.

- Individual*
- Device
- System
- Vendor

*If the account exists in the credential vault, the ownership type cannot be Individual. If the account is *not* available in the credential vault, the ownership type can be Individual. However, in this case, the owner changes, and the account is not added to the credential vault.

RESET_PASSWORD

Optional. Specifies whether the account password must be reset after adding the account to the credential vault. The valid values are TRUE and FALSE. The default value is FALSE.

PASSWORD

Optional. Specifies the password of the account.

USE_DEFAULT_SETTINGS

Optional. Specifies whether to apply the global default settings to the credentials. The valid values are TRUE and FALSE. If this setting is TRUE, then the other credential settings columns are ignored.

Note: In previous releases, this column header is called `USE_GLOBAL_SETTINGS`.

If this column is not specified, the value is set as follows:

- If none of the credential setting columns (`ACCESS_MODE`, `PASSWORD_VIEWABLE`, `MAX_CHECKOUT_DURATION`, `ENABLE_CHECKOUT_SEARCH`, `RESET_PASSWORD_ON_CHECKIN`) are specified, the `USE_DEFAULT_SETTINGS` value is set to `TRUE`.
- If at least one of the credential setting columns is specified, the credential will not use global default settings; the `USE_DEFAULT_SETTINGS` value is set to `FALSE`.

ACCESS_MODE

Optional. Specifies the access mode of credentials. You can use the following valid values:

- 0 indicates exclusive permissions. (Requires checkout and checkin.)
- 1 indicates nonexclusive permissions. (Does not require checkout and checkin.)
- 2 indicates nonshared credentials. (Credential is not shared.)

This setting is optional. If you do not specify a value, then the default value is 0 (exclusive).

PASSWORD_VIEWABLE

Optional. Specifies whether to display the credential password to users on the self-service user interface. You must specify this attribute if the access mode value is 0 or 1. The default value is `TRUE`.

MAX_CHECKOUT_DURATION

Optional. Specifies how long a credential can be checked out. Specify the time in weeks, days, or hours by adding the suffix, as described in the following examples:

- 8 w indicates eight weeks.
- 8 d indicates eight days.
- 8 h indicates eight hours.

If you do not specify a value, then the default time duration is 8 h.

ENABLE_CHECKOUT_SEARCH

Optional. Specifies whether the checkout search must be enabled for the credential on the self-service user interface. The default value is `TRUE`, which indicates that the checkout search is enabled for the credentials on the self-service user interface. To disable the checkout search for credentials, specify `FALSE`. This attribute is optional.

RESET_PASSWORD_ON_CHECKIN

Optional. Specifies whether the password must be reset on the self-service user interface after you check in a credential. The default value is `TRUE`, which indicates that the password is reset on the self-service user interface after you check in a credential. If you do not want the password to be reset after you check in a credential, specify `FALSE`.

DISCONNECT

Optional. Specifies whether to disconnect the credential from the account. Specify `TRUE` if you want to disconnect the credential from the account or `FALSE` if you do not want to disconnect.

When a credential is disconnected from the associated account:

- Users can still check out the credential, but the system cannot reset the password when the credential is checked back in.
- The account password is not synchronized to the credential vault when the account password is changed.

First example

The following sample CSV file contains information about the credentials to be added or updated in the credential vault:

Note: The following example data must be entered as two lines only. The example below is broken into multiple lines, in order to display correctly in PDF format. The only line break occurs after the column headers. In this example, the last column header is RESET_PASSWORD_ON_CHECKIN. The line breaks immediately after that word, and before the comma. To use this example, you must take out the line breaks that occur after OWNERSHIP_TYPE, ENABLE_CHECKOUT_SEARCH, and ,,,. In the correct format, the second line must include all characters from , "erglobalid= to the end of the data.

```
#Credentials
SERVICE_URI,SERVICE_PDN,SERVICE_ORG_CONT_URI,SERVICE_ORG_CONT_PDN,SERVICE_TYPE,ACCOUNT_UID,DESCRIPTION,OWNER_URI,OWNER_PDN,OWNERSHIP_TYPE,
RESET_PASSWORD,PASSWORD,USE_DEFAULT_SETTINGS,ACCESS_MODE,PASSWORD_VIEWABLE,MAX_CHECKOUT_DURATION,ENABLE_CHECKOUT_SEARCH,
RESET_PASSWORD_ON_CHECKIN
,"erglobalid=3204034161065175146,ou=services,erglobalid=000000000000000000,ou=org,dc=com",,,,Account1,"Account1 Description",,,
Device,false,pas$w0rd,false,0,true,6h,true,true
```

In the previous example, the SERVICE_PDN identifies a specific service, and the ACCOUNT_UID is Account1. IBM Security Privileged Identity Manager searches for the account and does one of these tasks:

- Adds the account to the credential vault with the specified settings if it is not currently in the credential vault and it is not an orphan account.
- Updates the credential settings with the specified value if it is currently in the credential vault.

Note: The owner columns are not specified. Therefore, the owner remains the same.

The shared access CSV file lists the column headers in a default sequence. You can change the sequence of these column headers according to your requirements. However, do not change the names of these column headers.

Second example

Note: The following example data must be entered as two lines only. The example below is split into multiple lines, in order to display correctly in PDF format. The only line break occurs after the column headers. In this example, the last column header is RESET_PASSWORD_ON_CHECKIN. The line breaks immediately after that word, and before the comma. To use this example, you must take out the line breaks that occur after OWNERSHIP_TYPE, ENABLE_CHECKOUT_SEARCH, and "description=testdec,o=Organization". In the correct format, the second line must include all characters from , "description=test to the end of the data.

```
#Credentials
SERVICE_URI,SERVICE_PDN,SERVICE_ORG_CONT_URI,SERVICE_ORG_CONT_PDN,SERVICE_TYPE,ACCOUNT_UID,DESCRIPTION,OWNER_URI,OWNER_PDN,OWNERSHIP_TYPE,
RESET_PASSWORD,PASSWORD,USE_DEFAULT_SETTINGS,ACCESS_MODE,PASSWORD_VIEWABLE,MAX_CHECKOUT_DURATION,ENABLE_CHECKOUT_SEARCH,
RESET_PASSWORD_ON_CHECKIN
,"description=test,l=NewYork,ou=Finance,o=Organization",,,WinLocalProfile,John Smith,"Test description",,"description=testdec,o=Organization",
Device,false,kk39kcDX,false,0,true,2d,true,true
```

IBM Security Privileged Identity Manager initially resolves to ORG_PDN to resolve to the SERVICE_PDN. The ORG_PDN is resolved to one or more organizational containers.

In the previous example, IBM Security Privileged Identity Manager resolves to the specified ORG_DN (l=New York,ou=Finance,o=Organization) in a particular manner. That is, IBM Security Privileged Identity Manager searches for the location New York that is located inside the organizational unit Finance under the organization Organization. From all the organizational containers that are obtained, IBM Security Privileged Identity Manager then searches for the services under the specified criteria. That is, it searches for all the services that have description as test.

Credential matching for the #Credentials type

IBM Security Privileged Identity Manager matches the credentials by account ID and service type if they are specified for all the services that are applicable. If the specified account for the specified service is in the vault, the specified credential settings update the credential. There can be single or multiple applicable services.

Services are resolved with one of the following data columns from the shared access CSV file in the sequence specified:

1. SERVICE_URI
2. SERVICE_PDN
3. SERVICE_ORG_CONT_URI
4. SERVICE_ORG_CONT_PDN

Note: When the data column of higher order is specified, the other columns are ignored. The data entry is not valid if none of the service columns are specified.

Credential matching for the #Credentials_v2 type

IBM Security Privileged Identity Manager matches the credentials by account ID and resource UID. If the credential service UID is not specified, IBM Security Privileged Identity Manager resolves the credential by account ID and service PDN.

Each CSV entry represents one credential. If the credential for the specified account UID and resource UID does not exist, the credential is created; otherwise, the credential settings are updated. If a credential exists in the vault and the specified password is different from the password that is stored in the vault, the credential password is also updated. If CONNECT_SERVICE_PDN is specified, the credential is connected to the account residing on the specified service.

Uploading a CSV file with the administrative console

As a privileged administrator, you can add or update the credentials or credential pools that are specified in the comma-separated value (CSV) file to the credential vault with the administrative console.

Before you begin

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

About this task

If a credential or credential pool exists in the credential vault, IBM Security Privileged Identity Manager uses the settings in the CSV file to modify the credentials or credential pools. If there is no setting change for a credential or credential pool, that entry is skipped.

Restriction: The maximum threshold of shared credentials in the CSV file is 1,000.

Procedure

To upload a CSV file, complete these steps:

1. From the navigation tree, click **Manage Shared Access > Shared Access Bulk Load**. The Upload CSV File page is displayed.
2. Optional: In the **Upload Name** field, type a name to identify the upload operation.
3. Click **Browse** to locate the CSV file that contains all the names of credentials to add to the credential vault.
4. Submit the request for uploading the CSV file in one of these ways:
 - To submit the request immediately, click **Submit Now**.
 - To submit the request later, click **Schedule Submission** to schedule the request to upload the CSV file in the future.

After you submit the request, a Success page is displayed that confirms that you completed your task. If the format of the CSV file is incorrect, you receive an error message. Correct the error and submit the request again.

Results

IBM Security Privileged Identity Manager adds all the credentials or credential pools that are specified in the CSV file to the credential vault.

What to do next

You can view the status of your request by selecting **View Requests** in the navigation tree. The tasks in **View Requests** provide detailed information about the request. Information includes the number of credentials that are added, modified, or failed because of incorrect values in the CSV file.

Configuring the credential default settings

Specify the default settings for each credential that is added to the credential vault.

Before you begin

You must be a system administrator to perform this task.

About this task

The administration console supports adding user credentials into a credential vault. When you add a credential to the vault, you can apply default values for each of the credential settings. Use this task to define the default value for each setting.

Note: Some default settings can be overwritten at the individual credential level, but others can be changed only at a global level.

Procedure

To configure the credential default settings, complete these steps:

1. From the navigation tree, select **Manage Shared Access > Configure Credential Default Settings**. The Configure Credential Default Settings page is displayed.
2. Under **Credential Setting**, select one of the following options to specify the check-in and check-out process for the accounts. See the online help for details about individual settings.

Require the check-in and check-out process for the shared IDs

Select this option to specify that by default users must check out a shared credential before they use it. When you select this option, specify the following options:

Change password upon checkin

Select the check box to change the password.

Note: For credentials that are not connected to an account, the credential password is not changed at check-in even if **Change password upon checkin** is enabled.

Maximum checkout duration

Schedule the maximum number of hours, days, or weeks that a credential can be checked out.

Specify whether the credential is enabled for checkout search

Select the **Enable checkout search** check box to enable the credentials for a check-out search. When you do so, the accounts are searched for the check-out process on the self-service user interface.

Specify whether the credential password is visible to the user in Self Service

Select the **Display the password to user** check box to display the credential password to the user on the self-service user interface.

Check Out Operation

In the **Operation Name** field, enter an operation name to define a global lifecycle operation and start the check-out workflow extension.

Lease Expiration Handling

Notify violation

Select this option to send a notification when the system finds the expired credentials that are checked out.

Notify violation and checkin

Select this option when you want the system to notify the recipients about the expired credentials and check in those credentials automatically.

Notification Template

Click this link to view or change the email template that is used by the system to construct the expired credential notification.

Send notification to

Select a recipient from the list.

Check for expired leases every

Schedule a time frequency that you want the system to check for the expired credential leases.

Note: The time that you enter must be equal to or greater than the time specified for checking expired leases. For example, you might set the interval of every 1 hour to check for expired leases. You must set at least every 1 hour or more to send notifications to the recipients who are responsible for the expired leases.

Send notifications at least every

Schedule a time frequency to send out notifications to remind the recipients of the expired leases.

Do not require the checkin and checkout process for shared IDs

Select this option to specify that, by default, users must not check out a shared credential before they use it.

Specify whether the credential password is visible to the user in Self Service

Select the **Display the password to user** check box if you want to display the credential password to the user on the self-service user interface.

Credential is not shared

Select this option if you do not want any user to access the credential by using a shared access policy. When you select this option, the credential is stored in the credential vault. However, the credential cannot be retrieved by using the IBM Security Privileged Identity Manager Shared Access Module.

3. Click **Submit** to save the configuration settings.
4. On the Success page, click **Close**.

Checkout operation customization

Shared Access Management supports both synchronous and asynchronous checkout of shared accounts. Synchronous checkout is enabled by default. If you want to use asynchronous checkout, you must enable and configure it.

To enable asynchronous checkout, you must define a global lifecycle operation to start the checkout workflow extension. You must also configure the operation name in the global settings for the shared access module.

IBM Security Privileged Identity Manager provides example code that shows you how to complete the configuration. The example shows how to define a checkout operation with or without RFI node followed checkout extension.

Define a checkout operation with the checkout extension

Configure the operation name in the Shared Access Management global setting.

Procedure

1. From the Administrative console, select **Configure System > Manage Operations**.
2. Select **Global level** for the **Operation Level** and click **Add**.
3. Enter a name for the operation and click **Continue**.

Note: The name you assign to this operation is required when configuring the Shared Access Management credential default settings.

4. In the Operation Diagram, click **Properties**.
5. In the Properties window' **Input Parameters** section, add the relevant data for credential, credential lease, account and person then click **OK**.
6. Add an **Extension** node in the Operation Diagram.
7. Right-click the **Extension** node and select **Properties**.
8. In the **Extension Name**, select **checkout(Credential credential, CredentialLease leaseIn, Account account, Person person)**.

Note: If you do not see the checkout extension, Shared Access Management is not enabled. Map the required input parameters and output parameters to the checkout operation relevant data. Select each input and output parameter and click **Search Relevant Data**. Map the corresponding relevant data to each parameter.

9. Save the operation.
10. From the Administrative console, select **Manage Shared Access > Configure Credential Default Settings**.
11. Specify the name of the operation you created in to the **Check Out Operation > Operation Name** field.

Results

The checkout task invokes the checkout operation that you created. To switch it back to synchronous mode, remove the operation name in the credential default settings.

Note: For the relevant data ID and activity ID, if you specify a different value from the example, you might want to define a label for the ID in the `CustomLabels.properties` file.

Define a checkout operation with an RFI node followed by the checkout extension

This example illustrates the scenario where a user checks out a credential to perform an administrative task, and the manager must provide a ticket number for that task. Credential lease object class has 5 pre-defined custom attributes, which can be mapped to any single-value string attributes. This example maps the first custom attribute to the ticket number.

Procedure

1. On top of the checkout operation in "Define a checkout operation with the checkout extension" on page 91, add an **RFI** node before the checkout **Extension** node.
2. Right-click the **RFI** node and select **Properties**.
3. Select the **General** tab and complete the required fields on the RFI node: Activity ID, Participant, Entity Type, Entity, and the attributes required for input from the participant.
4. Select the **Parameters** tab and map the input parameters to the relevant data ID defined at the operation level.
5. Select the **Notification** tab and deselect **Use Group Email Topic**. You can:
 - Use the default notification template or

- Deselect **Use Default Template** and customize the notification template by introducing new keys and defining new keys and labels in `customLabels.properties`.
6. Save the operation.
 7. Include the RFI attributes in the credential lease form.
 8. From the Administrative console, select **Configure System > Design Forms**.
 9. Select **Credential Lease** and add `ercustomattribute1` in the form.
 10. Save the form.
 11. Change the label of `ercustomattribute1` in `CustomLabels.properties` to be a Ticket Number.

Changing the operation name label

By default, the checkout request name under **View Requests** is shown as **Custom Operation**. To make it more user friendly, change the workflow ID in the process definition. You must manually change the process definition in the LDAP server.

Procedure

1. Locate the operation container `ou=operations,ou=itim,<Tenant DN>`.
2. Within the operations container, locate the new operation you created for checkout. Search for `erprocessname = <checkout operation>`.
3. Edit the `exXml` attribute value. Change the `WORKFLOWID` to `C0` instead of `CP` and save the entry. The label for process type `C0` is defined in `Labels.properties` `processType.C0`

```
<?xml version="1.0" encoding="UTF-8"?> <PROCESSDEFINITION NAME="checkout"
WORKFLOWID="C0" COUNTRY_KEY="US" .....
```

Shared access approval for adding credentials to the vault

You can add an approval process to the default operation for adding credentials to the vault.

IBM Security Privileged Identity Manager uses the existing lifecycle operation module to add credentials to the vault. The default operation `addCredentialToVault` does not include approval, but can be customized to incorporate approval activity.

IBM Security Privileged Identity Manager supports a single global operation that is used by all credentials, regardless of the services, service type, or the organizational unit to which the account belongs.

Customizing the checkout form

You can customize the form that is used for checkout of shared accounts. You can add more attributes to be filled out during checkout. This customization increases individual accountability when credentials are shared.

About this task

You must be a system administrator to complete this task. The checkout form is global for all shared access. When you customize the checkout form, your changes affect checkout for all shared access. Use this procedure to add or remove

attributes from the checkout form template.

Procedure

1. Log in to the administration console and select **Configure System > Design Forms**.
The Design Forms Java™ applet is displayed.
2. Optional: To open the applet in a separate browser window, click **Launch as separate window**.
3. In the left pane, double-click the “Credential Lease” category folder to select the “Credential Lease” form. Double-click the form to open it in the form designer.
4. Select **custom attribute** and then click the **Add Row** icon to add it to the form.
5. Click the correct icon to select the widget. Specify required attributes for each widget. Also, specify the format and constraints for each attribute.
6. Repeat the previous two steps to add all custom attributes.
7. Click the **Save Form Template** icon to save the changes. Click **OK**.
8. Optional: If you opened the Design Forms Java applet in a separate window, close the window.
9. Click **Close** to close the Design Forms applet.

Configuring the shared access credential usage prompt

Use an injection policy to configure the prompt that asks the user whether to use shared credentials. The prompt is displayed when you log on to a managed resource, when you use any of the client applications.

Before you begin

Enable the shared access policy on the user profile.

1. Log on to Single Sign-On administration console.
2. Under **User Policy Templates**, click **New template**.
3. Verify that Use Shared Credentials exists under Authentication Service Policies.
4. Click **Add**.
5. Apply the template to each user who requires the configuration of the prompt behavior for shared access. See "Applying a User Policy Template" in the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*.

Procedure

1. Open the Wallet Manager.
2. On the **Authentication Service** column, search for **Use shared credentials** and select any of the **Password Entry** options.

Table 6. Password entry options

Password entry	Description
Automatic logon	Use only shared credentials to log on to the managed resources.

Table 6. Password entry options (continued)

Password entry	Description
Always	<ul style="list-style-type: none">• Always asks the user to use shared credentials to log on or not.• Always use the selected IBM Security Privileged Identity Manager user.
Ask	<ul style="list-style-type: none">• Asks the user to use shared credentials to log on or not.• Asks for the IBM Security Privileged Identity Manager user.
Never	Do not use shared credentials to log on to the managed resources.

Configuring the reauthentication prompt

For more security, IBM Security Access Manager for Enterprise Single Sign-On users can be asked to reauthenticate when they access managed resources. Configure whether to require the users to reauthenticate every time that a user accesses a client application or command that requires shared credentials.

Procedure

1. Start the **AccessAdmin**.
2. Click **Authentication service policies**.
3. Select the authentication service **Use Shared Credentials**.
4. Under **Password Policies**, specify whether to require reauthentication before you single sign-on by using the automatic sign-on mode.

Chapter 7. Services administration

A *service* can be an identity provider, an identity feed service, or the built-in ISPIM service and TAM/ESSO service. An identity provider represents a user repository for a resource, such as an operating system, a database application, or another application that IBM Security Privileged Identity Manager manages. For example, a managed resource might be a Lotus Notes® application, and a service can be defined for a 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 Privileged 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 Privileged Identity Manager.

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

Identity-feed service administration tasks

Identity-feed service administration tasks are done by using **Manage Services** from the navigation menu. Service administration tasks include the following tasks:

- Creating services
- Changing or deleting services
- Scheduling a reconciliation

Related concepts:

“Identity provider management” on page 62

Identity providers let you manage passwords of privileged credentials that reside on resources, hosts, or network devices.

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 to access. Create one service for each Lotus Domino server with the Lotus Domino service type. In previous versions of IBM Security Privileged Identity Manager, a service type is called a *service profile*.

Some service types are installed by default when IBM Security Privileged 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 IBM Security Privileged Identity Manager adapter for a managed resource. There is a service type for each type of managed resource that IBM Security Privileged 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 IBM Security Privileged Identity Manager.

IBM Security Privileged 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 IBM Security Privileged 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 IBM Security Privileged 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 IBM Security Privileged 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 IBM Security Privileged Identity Manager and add or update users to IBM Security Privileged 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 IBM Security Privileged 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 IBM Security Privileged Identity Manager and to manage accounts in the IBM Security Privileged 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 IBM Security Privileged Identity Manager.

Identity provider service types:

Security Directory Integrator-based

This service type can be optionally installed during the installation of IBM Security Privileged 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.

ISPIM Service

The ISPIM service type is used to create accounts in the IBM Security Privileged Identity Manager system and represents the IBM Security Privileged Identity Manager itself. This type is a standard service with no configuration parameters. All users that need access to the IBM Security Privileged Identity Manager system must be provisioned with an IBM Security Privileged 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 Privileged 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 identity provider on the Manage Identity Providers panel.

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.

Creating identity feed services

Create an instance of a service from a service type, such as the DSML service.

Before you begin

Before you can create a service in IBM Security Privileged 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 Privileged 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

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.

Procedure

1. From the navigation tree, click **Manage Services**.
2. On the Services table, 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**.
6. On the Service Information page, specify the appropriate values for the service instance. The content of the Service Information page depends on the type of service that you are creating.
7. Click **Finish**.

Results

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

What to do next

Create another service or click **Close**.

Setting the service unique identifier

In the managed resource service definition, set the unique identifier for connecting to the managed resource. For example, the unique identifier might be an IP address or the host name of the server.

About this task

These steps must be performed for every service instance that you want to configure for shared access.

To set the unique identifier, you must complete the **Unique identifier** field that was configured in the service form template. For more information, see *Customizing the service form template to include the unique identifier (eruri) attribute* .

Procedure

To set the service unique identifier field, complete these steps:

1. Create or change the service that you want to configure for shared access.
 - To create a service, see “Creating identity feed services” on page 100.
 - To change a service, see “Changing identity-feed services” on page 103.
2. When you complete the General Information page, ensure that you complete the **Unique identifier** field that was created for shared access. Type the unique identifier for connecting to the managed resource. For example, the unique identifier might be an IP address or the host name of the managed resource. This field is used if you also use IBM Security Access Manager for Enterprise Single Sign-On for automatic checkout. IBM Security Access Manager for Enterprise Single Sign-On uses the field to locate the resource.

What to do next

Define access to grant ownership of sponsored accounts. For more information, see the following topics:

- “Creating roles” on page 238
- “Specifying owners of a role” on page 243

You can also 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.

Related tasks:

“Creating identity feed services” on page 100

Create an instance of a service from a service type, such as the DSML service.

“Changing identity-feed services” on page 103

You can change the information for a service instance.

“Customizing the service form template to include the unique identifier (eruri) attribute”

Update the managed resource service form template to include a field for the unique identifier that you use to connect to the managed resource.

Customizing the service form template to include the unique identifier (eruri) attribute

Update the managed resource service form template to include a field for the unique identifier that you use to connect to the managed resource.




About this task

You must perform these steps for every service type that you want to configure for shared access if you also use IBM Security Access Manager for Enterprise Single Sign-On for automatic checkout. The default forms for services, groups, and accounts are based on the adapter.

You must be a system administrator to perform this task.

Procedure

To add the eruri attribute to the service form template, complete these steps:

1. From the navigation tree, select **Configure System > Design Forms**. The **Design Forms** Java applet is displayed.
2. Optional: To open the applet in a separate browser window, click **Launch as separate window**.
3. In the left pane, double-click the **Service** category folder to display the object profiles.
4. In the left pane, double-click a profile, such as **POSIX Linux profile**, to open the template for that profile. The form template associated with the object profile is displayed in the middle pane.
5. In the **Attribute List** box, select the **eruri** attribute and then click the **Add Row**  icon. The \$eruri attribute is added to the form template.
6. Select the \$eruri attribute and then click the **Editable Text List**  icon. The \$eruri attribute is a multivalued attribute.
7. In the **Properties** box, type a new label name in the **Label** field. For example, type **Unique identifier**. The label name that you type here is displayed in the service form whenever you create or change a service that is based on this profile. For example, the label name is displayed in a POSIX Linux service that you create or change.
8. Click the **Save Form Template**  icon to save the changes, and then click **OK**.
9. Optional: If you opened the **Design Forms** Java applet into a separate window, close the window.
10. Click **Close** to close the **Design Forms** applet.

What to do next

Create a service instance from the profile, such as POSIX Linux, and complete the new **Unique identifier** field.

Related tasks:

Setting the service unique identifier

In the managed resource service definition, set the unique identifier for connecting to the managed resource. For example, the unique identifier might be an IP address or the host name of the server.

Creating services

Create an instance of a service from a service type, such as the DSML service.

Changing identity-feed services

You can change the information for a service instance.

Before you begin

Before you can change a service in IBM Security Privileged 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**.

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 page, change the appropriate values for the service instance, and then click **OK**.

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.

Deleting identity-feed services

Delete service instances when necessary.

Before you begin

Before you can delete a service in IBM Security Privileged 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 IBM Security Privileged 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.

Creating service types

As an administrator, you can create a service type. For example, you might create a service type for a manual service that you want to create.

Before you begin

Defining a new service type allows you to define new LDAP attributes and objectclasses. You can also change the existing LDAP attributes and objectclasses. You must understand the impact of changing the LDAP schema through this task. Do not change the syntax or schema of existing attributes and objectclasses. If a new service type is needed, define one. See your directory documentation for restrictions and best practices to use for schema extension. For IBM Security Directory Server Version 6.1, see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd13.htm#wq78.

About this task

You can create a service type for a manual service or for a custom service.

Procedure

1. From the navigation tree, select **Configure System > Manage Service Types**. The Manage Service Types page is displayed.
2. On the Manage Service Types page, click **Create**. The Manage Service Types notebook is displayed.
3. On the General page of the Manage Service Types notebook, complete these steps:
 - a. In the **Service Type Name** field, provide a unique name for your service type.
 - b. From the **Service Provider** list, select the protocol that IBM Security Privileged Identity Manager uses to provision accounts for the service type.
 - c. Click the **Service** tab.
4. On the Service page, specify an LDAP class and attributes to associate with the service type, and then click the **Account** tab. The LDAP class and attributes vary, depending on the accounts that the managed resource provides.

5. On the Account page, specify an LDAP class and attributes to associate with the account schema, and then click either the **Group** tab or **OK**.
6. Optional: On the Group page, complete these steps:
 - a. To add a group to the service type, click **Add**. The Add Group page is displayed.
 - b. On the Add Group page, specify an LDAP class and schema information. A group schema must be supported by the adapter for this service type.
 - c. Click either the **Miscellaneous** tab, or click **OK**.
7. Optional: On the Miscellaneous page, complete these steps:
 - a. Select the check box if you want the service type to participate in reports for dormant accounts.
 - b. From the **Last access date** list, select an attribute of the account schema that is associated with the service type, and then click **OK**.

Results

A message indicates that you successfully created a service type.

What to do next

Verify the generated service and account forms for the new service type with the form designer, set up account defaults for the service type, or click **Close**.

Tip: You can also specify values for **Service Type Name** and **Description** fields in the CustomLabels.properties file.

Changing service types

You can change a service type to select a different service provider. You can also change a service type to change the LDAP class or attributes for the service type or the accounts.

Before you begin

A service type must exist, but no instance of the service type can exist.

Defining a new service type allows you to define new LDAP attributes and objectclasses. You can also change the existing LDAP attributes and objectclasses. You must understand the impact of changing the LDAP schema through this task. Do not change the syntax or schema of existing attributes and objectclasses. If a new service type is needed, define one. See your directory documentation for restrictions and best practices to use for schema extension. For IBM Security Directory Server Version 6.1, see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd13.htm#wq78.

About this task

You cannot change a service type if there is a service instance of the service type. Users might actively be working in accounts on that service instance.

Procedure

1. From the navigation tree, select **Configure System > Manage Service Types**. The Manage Service Types page is displayed.

2. Manage Service Types page, select the check box next to the service type that you want to change, and then click **Change**. The Manage Service Types notebook is displayed.
3. On the Manage Service Types notebook, make the wanted changes, and then click **OK**. The name of the service type cannot be changed.

Results

A message indicates that you successfully modified the service type.

What to do next

If necessary, use the form designer to update the service and account forms to match any service type attribute changes, or click **Close**.

Importing service types

As an administrator, you can import a service definition file, which creates a service type. Service definition files are also called adapter profile files, which are provided with the various IBM Security Privileged Identity Manager adapters.

Before you begin

The file to be imported must be a Java archive (JAR) file.

About this task

You can create a service type for an adapter that provides a JAR file.

Procedure

1. From the navigation tree, select **Configure System > Manage Service Types**. The Manage Service Types page is displayed.
2. On the Manage Service Types page, click **Import**. The Import Service Type page is displayed.
3. On the Import Service Type page, complete these steps:
 - a. In the **Service Definition File** field, type the directory location of the file, or click **Browse** to locate the file. For example, if you are installing the IBM Security Privileged Identity Manager adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
 - b. Click **OK** to import the file.

Results

A message indicates that you successfully imported a service type.

What to do next

The import occurs asynchronously, which means it might take some time to complete. On the Manage Service Types page, click **Refresh** to see the new service type. If the service type is not displayed within a reasonable amount of time, check the log files to determine why the import failed.

Deleting service types

You can delete a service type that has no service instances. For example, if your enterprise replaces an application, you might migrate user records to the new application. Then, delete the obsolete service type.

Before you begin

Before you delete a service type, you must remove all of its service instances.

About this task

When you delete a service type, changes made to the LDAP class persist even after the service type is deleted.

Procedure

1. From the navigation tree, select **Configure System > Manage Service Types**. The Manage Service Types page is displayed.
2. Manage Service Types page, select the check box next to the service type that you want to change, and then click **Delete**. Selecting the check box at the top of this column selects all service types. The Manage Service Types notebook is displayed.
3. On the Confirm page, click **Delete** to delete the service type, or click **Cancel**.

Results

A message indicates that you successfully deleted the service type.

What to do next

Do other service type management tasks, or click **Close**.

Reconciliation for manual services

Initiate a reconciliation activity on identity-feed service

Before you begin

You must have completed the steps for configuring a manual service type to support groups. You must also have created a manual service instance before you begin this task.

About this task

The service instance creation steps allow you to perform a reconciliation of a manual service using a comma-separated value (CSV) file that you provide. The reconciliation populates IBM Security Privileged Identity Manager with accounts and groups that exist on the manual service. The CSV file contains group and account information.

You can provide the reconciliation file at service creation time or at any time the service is modified. There is also a *supporting data only* option for reconciliation that is used when you want to pull group information from the CSV file, but you do not want to touch accounts in IBM Security Privileged Identity Manager.

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 the search should be performed against services or business units.
 - c. Select a service type from the **Search type** list, and then click **Search**. A list of services matching 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 performed on the service, and then click **Change**. The tasks that you can perform are dependent on the type of service. The Select Query page is displayed.
4. 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 or not to reconcile only supporting data.
5. Click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully submitted a reconciliation request.

What to do next

To view the results of the reconciliation, click **View the status of the reconciliation request**. You can also select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.

Creating a reconciliation schedule

You can schedule a reconciliation for identity-feed service.

Before you begin

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 Privileged 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

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

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.

Chapter 8. Group administration

IBM Security Privileged Identity Manager provides predefined groups. You can also create and modify customized groups.

Creating groups

A group represents a privilege in IBM Security Privileged Identity Manager. It determines set of tasks a IBM Security Privileged Identity Manager user can perform.

Before you begin

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 IBM Security Privileged Identity Manager service before creating a group. If the group does not previously exist, the access control item does not have the intended membership.

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 Groups**. The Select Group page is displayed.
2. In the **Groups** table, click **Create**. The Create Group page is displayed.
3. In the Create Group wizard, complete these steps:
 - a. 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 any members to the group.
 - b. Optional: On the Group Membership page, add members to the group, and then click **Next** to display the Schedule Add Member Operation page.
 - c. 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 IBM Security Privileged Identity Manager service, you can create an access control item to associate with this group.

Adding members to groups

You can add members to groups.

Procedure

To add members to a group, complete these steps:

1. From the navigation tree, click **Manage Groups**. The Select Group page is displayed.
2. On the Select Group page, type the information about the group in the **Search information** field.

In the **Search by** field, specify whether the search is done against group name or descriptions, or business units 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**.

3. In the **Groups** table, click the icon (▶) next to the group, and then click **Add Members**. The Add Members page is displayed.
4. On the Add Members page, complete these steps:
 - a. Type information about the user in the **System account information** field.
 - b. In the **Attribute** field, specify whether the search is done against user name or user ID, 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.
5. 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.
6. 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.

Procedure

To remove members from a group, complete these steps:

1. From the navigation tree, click **Manage Groups**. The Select Group page is displayed.
2. On the Select Group page, type the information about the group in the **Search information** field.

In the **Search by** field, specify whether the search is done against group name or descriptions, or business units 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**.
3. In the **Groups** table, click the icon (▶) next to the group, and then click **Manage Members**. The Manage Member page is displayed.
 4. 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.
 5. 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.
 6. 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

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 Groups**. The Select Group page is displayed.
2. On the Select Group page, type the information about the group in the **Search information** field.

In the **Search by** field, specify whether the search is done against group name or descriptions, or business units 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**.

3. In the **Groups** table, select the group that you want to modify, and then click **Change**. The Change Group page is displayed.

4. On the Change Group page, take the following actions:

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.

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**.

Deleting groups

You can delete groups from an ISPIM service.

About this task

You cannot delete a group that has members. 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 Groups**. The Select Group page is displayed.
2. On the Select Group page, type the information about the group in the **Search information** field.

In the **Search by** field, specify whether the search is done against group name or descriptions, or business units 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**.

3. In the **Groups** table, select one or more groups that you want to delete, and then click **Delete**. A confirmation page is displayed.
4. On the Confirm page, click **Delete**. A page is displayed, indicating that the delete operation was successful.

Results

The group is deleted.

What to do next

You can continue working with groups, or click **Close**.

Chapter 9. Policy administration

For your organization, you can manage policies, which are sets of organizational rules and logic.

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 Privileged 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, IBM Security Privileged 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

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 NT service instance overrides a password policy for the Windows NT service).

Procedure

1. From the navigation tree, select **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 Privileged 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**.

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.

Procedure

1. From the navigation tree, select **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 Privileged 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.

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 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 Privileged 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 rule

An administrator can change a password policy rule. For example, you might change or remove the settings for an existing rule.

Procedure

1. From the navigation tree, select **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 Privileged 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.

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 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 Privileged 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 Privileged Identity Manager Server and existing passwords.

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 Privileged Identity Manager Server.

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 Privileged 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 constraints 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 Privileged 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 Privileged 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 Privileged Identity Manager interprets the specified integer value for the rule in hours. IBM Security Privileged 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.

- IBM Security Privileged 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, IBM Security Privileged 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.

- IBM Security Privileged Identity Manager does not evaluate the rule when users change the password on accounts that are not owned by them. For example, IBM Security Privileged Identity Manager does not evaluate the rule when help desk or system administrators change the password on some other user accounts. IBM Security Privileged 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.
- IBM Security Privileged 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 IBM Security Privileged Identity Manager does not evaluate the rule correctly.

- IBM Security Privileged Identity Manager stores the password change information only when the password change is initiated by using one of these resources:
 - IBM Security Privileged Identity Manager console
 - IBM Security Privileged Identity Manager self service user interface
 - IBM Security Privileged 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.

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: `$ISPIM_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 `$ISPIM_HOME/data/CustomLabels.properties` file.

Note: `ISPIM_HOME` is the directory where IBM Security Privileged 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 `$ISPIM_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: `$ISPIM_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.

Creating a user policy template only for privileged identity management users

The shared access credential usage prompt can be configured for each group of users using user policy templates in AccessAdmin.

Procedure

1. Log on to AccessAdmin.
2. Create or modify an existing user policy template for privileged identity management users.
 - a. Under **User Policy Templates**, click **New template**.
 - b. Type a name for the template. For example: PIM admins only.
 - c. Expand the **Authentication Service Policies** group.
 - d. Expand **Use Shared Credentials**.
 - e. For **Password entry of injection policy per authentication service**, choose **Ask**.
 - f. Click **Update**.
 - g. Apply the user policy template to privileged identity management users. See the topic “Applying a User Policy Template” in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.
3. Create or modify an existing user policy template for non-privileged identity management users. For example: Non-PIM users only.
 - a. For the policy template, expand **Authentication Service Policies**.
 - b. Expand **Use Shared Credentials**.
 - c. For **Password entry of injection policy per authentication service**, choose **Never**.
 - d. Click **Update**.
 - e. Apply the user policy template to users that are not using privileged identity management. See the topic “Applying a User Policy Template” in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Chapter 10. Workflow management

Workflows for entitlements to an access can be added, deleted, and modified from the workflow design page. Additionally, you can change workflow properties, escalation, notification, and other workflow activities.

Adding an entitlement workflow

As an administrator, you can create a workflow for an access request.

Before you begin

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 for an access request.

Procedure

1. From the navigation tree, select **Configure System**. Then, 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. 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	<p>Click to add a workflow that consists of a linear series of approval, mail, or request for information activities.</p> <p>Complete the activity name, participant type, and escalation time and escalation participant type. Then, click OK.</p>
Advanced	<p>Click to add an advanced workflow potentially consisting of other types of activities, loops, and conditional branches. The workflow designer applet starts.</p> <p>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.</p>

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 an access request.

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 an access request.

Procedure

1. From the navigation tree, select **Configure System**. Then, 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 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 an access request.

Before you begin

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 **Configure System**. Then, 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 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.

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	<ol style="list-style-type: none"> 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	<p>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.</p> <p>a. In the General tab, make these entries:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>If you load a template, complete these tasks:</p> <ul style="list-style-type: none"> • 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. <p>c. In the Postscript tab, type any postscript information.</p> <p>d. Click OK to complete the task.</p> <p>Depending on the customized steps that you took or the template that you selected, you might need to change the notification recipient.</p>

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 Privileged Identity Manager

IBM Security Privileged 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 Privileged 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 Privileged 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 Privileged 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.

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.

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.

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.

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.

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.

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.

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"><PARAM>
<JS> if (process.canceledDate != null) return process.canceledDate.getTime(); else return '';</JS></PARAM></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"><PARAM>
  <JS>if (process.canceledDate != null) return process.canceledDate.getTime();
  else return '';</JS>
  </PARAM></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 163

You can cancel requests that are not completed.

“Changing a workflow notification template” on page 135

You can use the Workflow Notification Properties page to change a workflow notification template.

Sample workflows

This section contains sample workflows.

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.

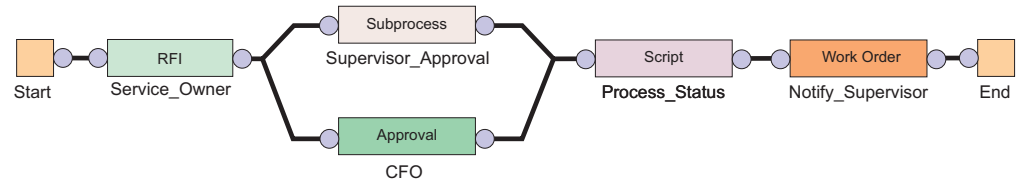


Figure 2. Sample workflow: multiple approvals required

Table 7. 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
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

Table 7. Node properties: Sample workflow for multiple approvals (continued)

Node	Feature	Value
Script	Activity ID	Process_Status
	Join Type	AND
	Split Type	AND
	JavaScript	<pre> supervisorApproval= process.getActivity("Supervisor_Approval").resultSummary cfoApproval=process.getActivity("CFO").resultSummary if(supervisorApproval==activity.APPROVED && cfoApproval==activity.APPROVED) { process.setResult(process.APPROVED) } else { process.setResult(process.REJECTED) } </pre>
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 Service_Owner RFI > 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
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.

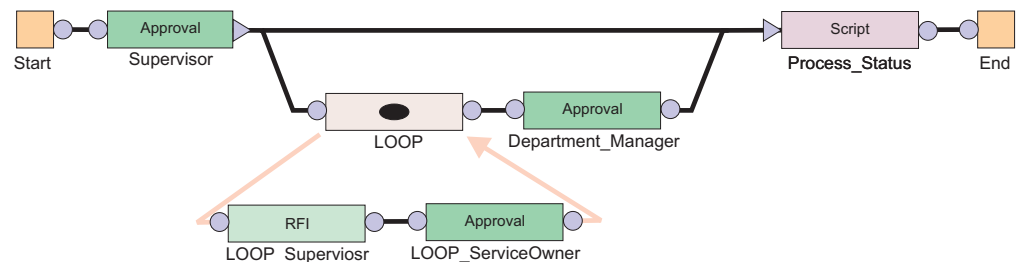


Figure 3. Sample workflow: multiple approvals with loop processing

Table 8. Node properties: Sample workflow for multiple approvals with loop processing

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A

Table 8. Node properties: Sample workflow for multiple approvals with loop processing (continued)

Node	Feature	Value
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
	Approval	Name
Participant		[Organizational Role] Department_Manager
Escalation Participant		System Administrator
Escalation Limit		1 day
Join Type		AND
Split Type		AND
Entity Type		Account

Table 8. Node properties: Sample workflow for multiple approvals with loop processing (continued)

Node	Feature	Value
Script	Activity ID	Process_Status
	Join Type	OR
	Split Type	AND
	JavaScript	[Custom] <pre> 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) } } </pre>
End	Activity ID	End
	Join Type	AND
	JavaScript	N/A
Transition LineStart > Supervisor Approval	JavaScript	[Custom] true
Transition LineSupervisor Approval > LOOP	JavaScript	[Approved] activity.resultSummary==activity.APPROVED;
Transition LineSupervisor 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		
Transition LineLOOP > Department_Manager Approval	JavaScript	[Custom] true
Transition LineDepartment_Manager Approval > Process_Status Script	JavaScript	[Custom] true
Transition LineProcess_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.

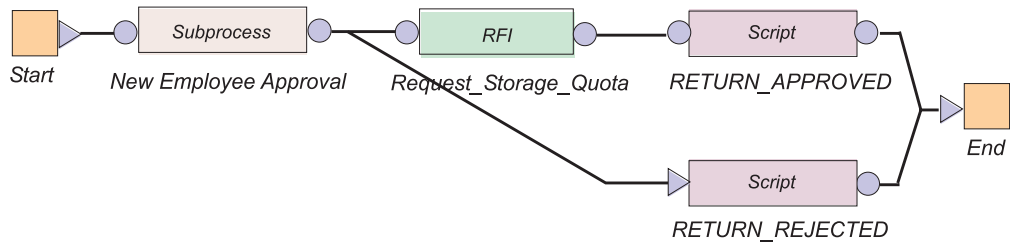


Figure 4. Sample workflow: RFI and subprocess

Table 9. 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
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	<code>process.setResult (process.APPROVED);</code>

Table 9. Node properties: Sample workflow with an RFI and a subprocess (continued)

Node	Feature	Value
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	OR
	Split Type	OR
	JavaScript	<code>process.setResult (process.REJECTED);</code>
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] <code>activity.resultSummary ==activity.APPROVED;</code>
Transition Line New Employee Approval > RETURN_REJECTED	JavaScript	[Rejected] <code>activity.resultSummary ==activity.REJECTED;</code>
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.

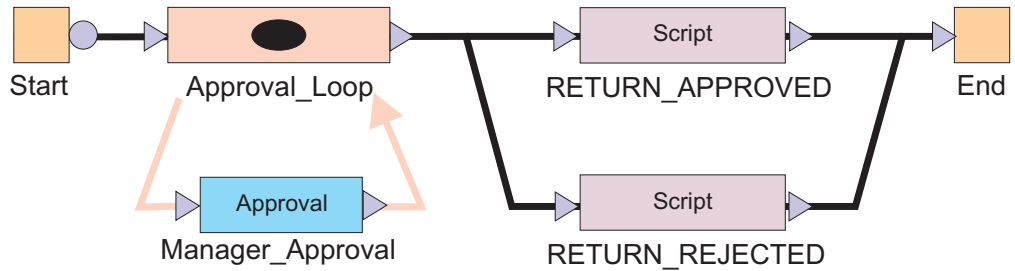


Figure 5. Sample workflow: approval loop

Table 10. 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);
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A
Transition LineStart > Approval Loop	JavaScript	[Custom] true

Table 10. Node properties: Sample workflow with an approval loop (continued)

Node	Feature	Value
Transition LineApproval Loop > RETURN_APPROVED	JavaScript	[Custom] approvalFlag.get() == "APPROVED"
Transition LineApproval 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: 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 `${ITIM_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.

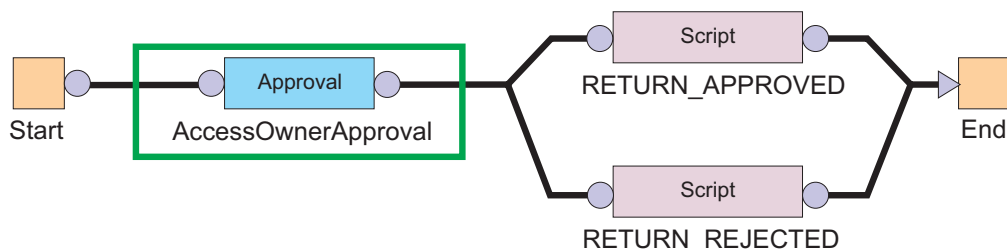


Figure 6. Sample workflow for access request

Table 11. 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
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 11. 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 12 describes each approval activity state.

Table 12. 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 13. 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.

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 Express®/IBM Security Privileged Identity Manager/IBM Security Identity Manager for z/OS®.

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 14 on page 152 gives a description of each work order state.

Table 14. 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.

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.

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.

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.

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.

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.

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.

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**.

Locking an activity

You can lock activities so others cannot act on them.

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.

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.

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.

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.

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.

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 12. 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 15. 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 15. 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.

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.

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.

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**.

Canceling pending requests

You can cancel requests that are not completed.

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**.

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 135

You can use the Workflow Notification Properties page to manually add information about canceling a request to the email notification template.

Related reference:

“Request for information (RFI) states” on page 151

When you view the status of a request, the request for information (RFI) activities might be in one of several states.

Chapter 13. Session recording administration

The IBM Privileged Session Recorder captures user activity of sessions on managed workstations.

Recording policies

You can use AccessAdmin to customize recording settings. You can customize settings such as recording quality, and keylogging enforcement.

Use AccessAdmin to configure the privileged session recording policies. See Policies for ESSO Agent.

Accessing recordings

You can access session recordings to play back, investigate, or audit the recorded usage of privileged identities.

Logging on to the IBM Privileged Session Recorder console

To log on to the Privileged Session Recorder console, the user must be a member of **Session Recording Auditors** group. You can also allow other groups to access this console by enabling the **View Recordings** task in the administrative console.

Before you begin

Grant security auditors access to the Privileged Session Recorder console. For more information, see Adding security auditors.

Procedure

1. Open the Privileged Session Recorder console at `https://<hostname>/recorder/ui`. For example: `https://pimva.example.com/recorder/ui`
2. Enter your credentials.
The Privileged Session Recorder console is displayed.

Searching for recordings

Use the available search and filter controls to find the session recording that you want to play back.

About this task

You can:

- Search recordings by their metadata, such as the user ID, application, or custom metadata.
- Search for commands entered in text-based recordings.
- Save frequent searches for faster access the next time you log on.

Table 16. What you can search for in recordings

What you can search for	Text-based recordings	Screen-based recordings
General Search capabilities		

Table 16. What you can search for in recordings (continued)

What you can search for	Text-based recordings	Screen-based recordings
	Commands that were entered on the managed UNIX endpoint session.	Not applicable
	Application name, IP address, and other session metadata.	
Advanced Search attributes		
User ID	The IBM Security Privileged Identity Manager user who signed on to a system.	
Local user ID	The Windows user who logged on a client computer.	
Application User ID	The privileged credential Login ID.	
Local host	Host name of the client computer.	
Service Host	The system that is accessed by using the privileged credential.	
Application name	The program on the user computer where the privileged credential is used.	
Process name	The executable file name of the application.	
Start Time	The date and time when the recording started on the client workstation. The time is displayed in the browser's time zone.	
End Time	The date and time when the recording ended on the client workstation. The time is displayed in the browser's time zone.	
Live recordings only	Recordings that have not ended.	
Terminal Command	The commands that were captured in the UNIX endpoint session. This attribute does not apply to session recordings with mainframe applications.	Not applicable

Saving frequently used search queries

If you repeat searches with specific criteria frequently, you can save your search queries for faster result retrieval.

About this task

Search queries that you save are shared with all the Privileged Session Recorder console users.

Procedure

1. In the Privileged Session Recorder console, use the **Advanced search** fields to refine and combine different search criteria.
2. Click **Saved searches**.
3. Specify a name for the saved search. For example: Linux endpoints in the last 30 days

Recording Permalink

Each recording is identified by a recording ID.

If you know the recording ID of the recording that you need to play back, you can access it directly using a permalink in the following format:

```
https://<hostname>/recorder/ui/SessionRecordingContainer.html?
recordingID=<recording_id>
```

For example:

Playing back recordings

Play back recordings from the IBM Privileged Session Recorder console to review the activities that occurred during a session.

Before you begin

To play a recording that is archived, you might need to contact your database administrator. To restore the archived recording, make a note of the part name from the notification message. If you have permissions to restore an archived recording, see “Restoring an archived recording” on page 170.

About this task

The following playback controls are available when you view recordings.

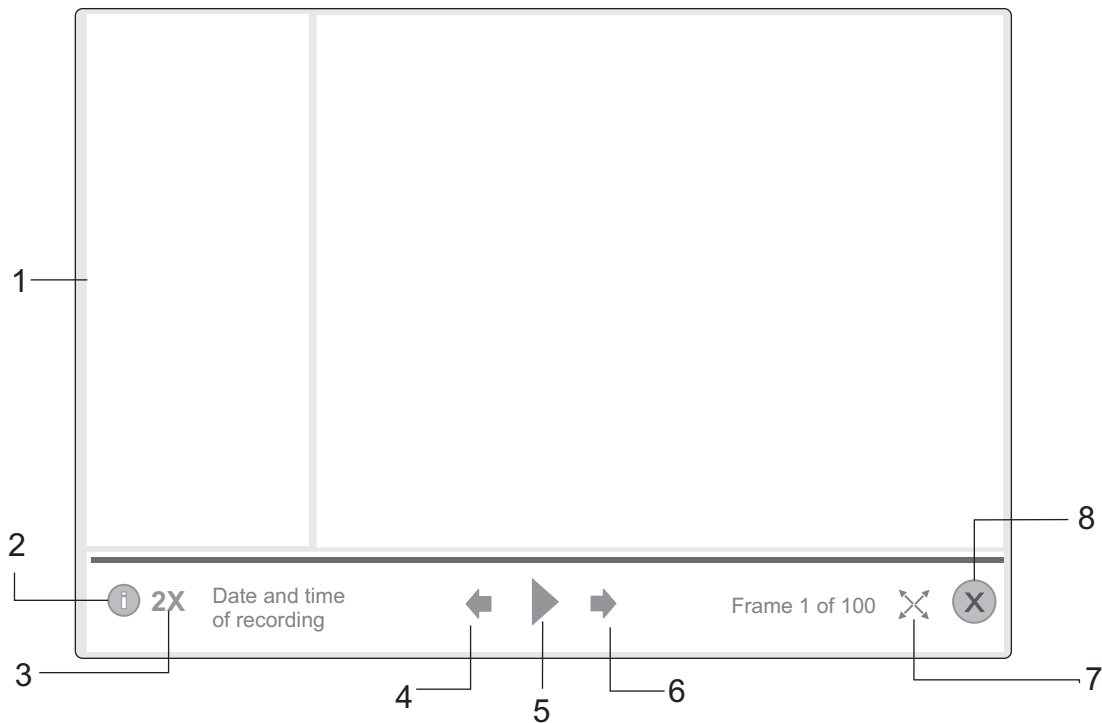


Figure 7. Playback and view controls

Table 17. Advanced playback and view controls

Item	Name	Description
1	Sidebar	Information Displays details about the recorded session, such as the IP address, date, and application. Commands Displays, in chronological order, the commands that were typed during the recording session. This control applies to text-based recordings only.

Table 17. Advanced playback and view controls (continued)

Item	Name	Description
2	Sidebar switch	Toggle the display of the information sidebar on or off.
3	Speed multiplier	Control the playback rate with the playback speed multiplier control. Each frame in a recording is played for the same amount of time, regardless of the delay between user actions.
4	Previous	Show the previous frame.
5	Play	Play the recorded session
6	Next	Show the next frame.
7	Full screen	View the recording in full screen.
8	Close	Close the player view.

Procedure

1. Log on to the Privileged Session Recorder console.
2. Search or filter the recordings that are based on the required fields.
3. Select the recording. Do one of the following steps:
 - Click **View recording**.
 - Double-click the recording.
4. Click **Play**.

Customizing the columns displayed

You can show or hide different columns in the Privileged Session Recorder console view. You can also rearrange the columns that are displayed.

Procedure

1. Log on to the Privileged Session Recorder console.
2. Click **Customize View**.
3. In the session recording view, complete any of the following tasks:
 - Click the **Plus** or **Minus** symbols to add or remove a column from the view.
 - Click the **Up** or **Down** arrows to change the order of columns displayed.

Note: You can also drag and drop the columns to change the order.

4. Save the view.

Database archival

Archive recordings periodically by moving them to a file-based storage based on online data retention policies. Regular archival ensures that recording storage space is manageable.

Each time the archival process runs, files are written to a directory that you specified. The database administrator can then choose to move the archived files to a remote storage location.

As a security analyst, you can still search for recordings that are archived. To restore archived recordings, the security analyst can provide the database administrator with the necessary parameters for archive retrieval.

Archiving the database

Archive recordings to save storage space.

About this task

Replace the following variables with values that apply to your deployment:

<psr_db>

Your Privileged Session Recorder database.

<user_name>

The database schema owner.

<part_name>

The partition that is selected for archiving for all the tables. For example: PART1.

<part_alias>

An alternative name for the partition that is selected for archiving. For example: ArchMarch2014.

Note: Each of the stored procedures include instructions that you can access from the DB2 command processor. For example, type `call sp_detach_partitionset('HELP')`.

Procedure

1. Open the DB2 command processor.
2. Connect to the Privileged Session Recorder database.
`DB2 CONNECT TO <psr_database> USER <db_owner> USING <password>`
3. View the partition list and select the partition to archive.
 - a. Enter the following command to see a list of partitions that can be archived.
`db2 call sp_list_archivable_partitionsets('EXECUTE')`

For example:

PARTID	PARTNAME	STARTTIME	ENDTIME
1	PART1	'2013-07-30-00.00.00.000000'	'2013-09-30-00.00.00.000000'
2	PART2	'2013-09-30-00.00.00.000000'	'2013-11-30-00.00.00.000000'

- b. Make note of the partition name that you plan to archive.
4. Detach the partitions into temporary tables.
 - a. Simulate detaching the partition.
`db2 call sp_detach_partitionset('SIMULATE',<partid>,<part_name>,<part_alias>')`
For example:
`db2 call sp_detach_partitionset('SIMULATE',1,'PART1','ArchMarch2014')`
This command checks whether the partition can be detached successfully.
 - b. Execute detaching the partition.
`db2 call sp_detach_partitionset('EXECUTE',<partid>,<part_name>,<part_alias>')`
For example:
`db2 call sp_detach_partitionset('EXECUTE',1,'PART1','ArchMarch2014')`
 5. Prepare the archive directory.
 - a. Create an empty directory for the archive, <archive_dir>. The directory must not contain spaces in the name. For example: `C:\archive`

- b. In the archive folder, create a folder with the name frames. For example:
C:\archive\frames
- c. In the archive folder, create a folder with the name images. For example:
C:\archive\images
- d. Ensure that the database user has permissions to write to this directory.

Important: The archive directory that you export to must exist before you enter the next set of commands in this task.

6. Export data from temporary tables to the archive directory.
 - a. Simulate exporting the data.

```
db2 call sp_archive_partitionset('SIMULATE','<part_alias>',
'<archive_folder_path>')
```

 For example:

```
db2 call sp_archive_partitionset('SIMULATE','ArchMarch2014',
'C:\archive')
```
 - b. Export the data.

```
db2 call sp_archive_partitionset('EXECUTE','<part_alias>',
'<archive_folder_path>')
```

 For example:

```
db2 call sp_archive_partitionset('EXECUTE','ArchMarch2014',
'C:\archive')
```

7. Check the archive directory and the exported files.
8. Delete the temporary tables.

CAUTION:

If you run this script before export is complete or if partition data is only partially exported, you cannot recover the partition data.

- a. Simulate pruning the detached partition.

```
db2 call sp_prune_detached_partitionset('SIMULATE', '<part_alias>')
```

 For example:

```
db2 call sp_prune_detached_partitionset('SIMULATE', 'ArchMarch2014')
```
- b. Prune the detached partition.

```
db2 call sp_prune_detached_partitionset('EXECUTE', '<part_alias>')
```

 For example:

```
db2 call sp_prune_detached_partitionset('EXECUTE', 'ArchMarch2014')
```

Restoring an archived recording

If a recording is already archived and you want to play it back, you must obtain the part name of the archived recording.

Before you begin

You must have database administrator privileges.

Procedure

1. Open the DB2 command processor.
2. Connect to the Privileged Session Recorder database.

```
DB2 CONNECT TO <psr_database> USER <db_owner> USING <password>
```
3. Load the archived partitions.
 - a. Simulate loading the archived partition.

```
db2 call sp_load_archived_partitionset('SIMULATE','<part_alias>',
'<archive_folder_path>')
```

For example:

```
db2 call sp_load_archived_partitionset('SIMULATE','ArchMarch2014',
'C:\archive')
```

b. Enter the command:

```
db2 call sp_load_archived_partitionset('EXECUTE','<part_alias>',
'<archive_folder_path>')
```

For example:

```
db2 call sp_load_archived_partitionset('EXECUTE','ArchMarch2014',
'C:\archive')
```

4. Mount the archived partition set.

a. Simulate mounting the archived partition set.

```
db2 call sp_mount_archived_partitionset('SIMULATE','<part_alias>',
'<part_name_mount>')
```

For example:

```
db2 call sp_mount_archived_partitionset('SIMULATE','ArchMarch2014',
'PART1_MNT')
```

b. Enter the command:

```
db2 call sp_mount_archived_partitionset('EXECUTE','<part_alias>',
'<part_name_mount>')
```

For example:

```
db2 call sp_mount_archived_partitionset('EXECUTE','ArchMarch2014',
'PART1_MNT')
```

5. Unmount the archived partition set.

a. Simulate unmounting the detached partition set.

```
db2 call sp_unmount_archived_partitionset('SIMULATE','<part_alias>')
```

For example:

```
db2 call sp_unmount_archived_partitionset('SIMULATE','ArchMarch2014')
```

b. Enter the command:

```
db2 call sp_unmount_archived_partitionset('EXECUTE','<part_alias>')
```

For example:

```
db2 call sp_unmount_archived_partitionset('EXECUTE','ArchMarch2014')
```

6. Prune the detached partition set.

a. Simulate pruning the detached partition set.

```
db2 call sp_prune_detached_partitionset('SIMULATE','<part_alias>')
```

For example:

```
db2 call sp_prune_detached_partitionset('SIMULATE','ArchMarch2014')
```

b. Enter the command:

```
db2 call
sp_prune_detached_partitionset('EXECUTE','<part_alias>')
```

For example:

```
db2 call sp_prune_detached_partitionset('EXECUTE','ArchMarch2014')
```

Adding a partition set

You must add a partition set when the end date for range of partitions is near. The virtual appliance set up process creates monthly partitions for a year. You must complete this task towards the end of the year.

Before you begin

You must have database administrator privileges.

Procedure

1. Open the DB2 command processor.
2. Connect to the Privileged Session Recorder database.
DB2 CONNECT TO <psr_database> USER <db_owner> USING <password>
3. To create a partition, choose one of the following ways:

call sp_create_psr_partitionset('EXECUTE', n)

Creates one instance of a new partition with a period of one month, where **n** is the number of months.

call sp_create_psr_partitionset('EXECUTE', 1, '<part_name>')

Creates one instance of a new partition set with a period of one month where <part_name> is a custom partition set name.

Chapter 14. Application identity management

Application administrators can use Privileged Identity Manager for Applications (App ID) to remove hardcoded and unsafely stored credentials from applications and scripts. App ID can also be used to manage the credential entitlements for each application, track the use of each credential, and automate periodic password change.

The App ID toolkit is provided to register applications and to allow different types of applications to get credentials that are managed by IBM Security Privileged Identity Manager.

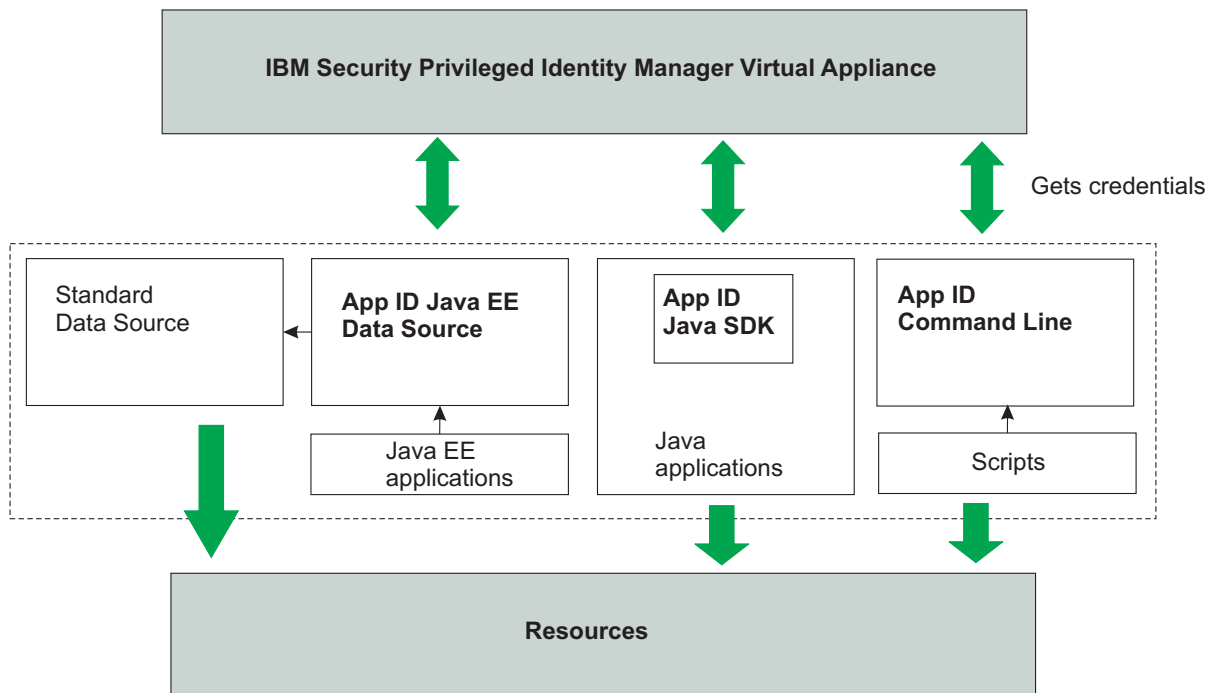


Figure 8. Application identities are often embedded inside data sources, custom applications, or unattended scripts to retrieve sensitive information.

Application identity management helps application and IT administrators accomplish the following goals:

- Remove hard-coded and unsafely stored passwords from applications, scripts, application servers, and their configuration files.
- Automatically change passwords.
- Remove access from applications that no longer require access to a resource.

IBM Security Privileged Identity Manager domain administrators can register application instances using the App ID toolkit and manage their credential entitlements using the Service Center. Registered instances use OAuth 2.0,

enhanced with secure application instance fingerprinting, to authenticate with the IBM Security Privileged Identity Manager Server.

An application may have multiple instances. For example, a Java EE application called HR Management System can be installed in Production Server, Staging Server, and Disaster Recovery Server. In App ID, each of these three install bases is called an *application instance*. The software, HR Management System, is called an application. Each application instance has a unique OAuth 2.0 access token and instance fingerprint. All instances of an application share the same set of credential entitlements.

An *application instance* is a IBM Security Privileged Identity Manager user. Unlike regular users, application instances cannot log in using a password.

The following steps describe the general process of enrolling a new application instance to use managed application identities.

1. Add the application credentials to the vault.

Note: Credentials for applications must be set to not require check-out. See “Specifying non-exclusive shared access credentials” on page 49.

2. Make the required modifications to the application code or the application server configuration.
3. Authorize the application instance.
4. Configure the credential entitlements for the application.
5. Verify that the application instance is able to fetch the credentials it requires.

Application instance fingerprint

The application authorization process captures specific properties that are used to form an application instance fingerprint. Attributes include the workstation that it is run from, the binary path, network configuration, and the operating system. A custom group name can be added to an instance's fingerprint.

The authorization process of an application captures the following attributes:

Table 18. Properties that can be used for fingerprinting with different application types.

Property	Compiled Application	Scripts	Java EE Application
Host name	Yes	Yes	Yes
Operating System User	Yes	Yes	Yes
Group Name	Yes	Yes	Yes
Host Time Zone	Yes	Yes	Yes
Network Interfaces	Yes	Yes	Yes
Operating System	Yes	Yes	Yes
Architecture	Yes	Yes	Yes
Binary Path	Yes	No	No
Binary Hash	Yes	No	No

Host name

Full qualified name of the instance host.

Operating system user

Name of the operating system user who runs the application instance.

Group name

The group ID of the application instance.

Host time zone

Time zone name of the instance host.

Network interfaces

All network interfaces in the host. Only the interface used to connect to the Privileged Identity Manager server will be used for fingerprint matching.

Operating system

Name of the operating system host.

Binary path

The path to the JAR file containing the class that uses AppIDManager.

Binary hash

SHA 256 hash value of the file that is specified in the **Binary Path**.

An application administrator can change the way an application instance's fingerprint is verified based on the organization's security requirements. An application administrator can choose the fingerprint matching policy for each application instance, which will determine the list of properties that are used for fingerprint matching. For example, to allow for convenient upgrades, an application administrator can select the "Environment" fingerprint matching policy, which will disable binary hash matching.

The following fingerprint matching policies are available:

Strict (default)

All properties are included in fingerprint matching. Ideal for scripts and applications using data source, as well as Java applications that seldom changes.

Environment

Binary hash is excluded from fingerprint matching. Ideal for applications that are updated frequently.

Flexible

Only group name, host time zone, and operating system are included. Ideal for virtualized environments.

Disabled

An application instance is allowed to get credentials as long as it presents the correct OAuth 2.0 tokens. This option can be used for disaster recovery instances that are then suspended until they are required.

App ID Toolkit

An application administrator or developer uses the App ID Toolkit to register application instances and enable them to retrieve managed credentials from the IBM Security Privileged Identity Manager Server.

The App ID Toolkit consists only of one file, `ibmappid.jar`. This file is used in three ways:

Command Line Tool

Run this file using the command `java -jar ibmappid.jar`. This command

line tool is used by the application administrator registering an application instance and by registered scripts to retrieve managed credentials.

Java SDK

Use the AppIDManager class in the `com.ibm.ispim.appid.api` package to enable a Java application to retrieve managed credentials

Java EE Data Source

Copy the file to your application server and configure a data source to be used by Java EE applications.

The App ID toolkit requires a workspace to store token files, SSL certificates of the server, and log files. By default, the workspace is the folder where the toolkit is located. Both the administrator who registers the application instance and the operating system user where the application instance runs must have read and write permissions to the workspace folder.

Note: The App ID toolkit requires a compatible Java runtime. Check the supported versions of Java in Software Product Compatibility Report.

Providing managed credentials to a script

You can modify scripts to use the App ID Command Line Tool to retrieve managed credentials from the IBM Security Privileged Identity Manager Server.

Before you begin

- Install a compatible version of Java Runtime Environment on the computer where the script runs.
- Add the application credential as a non-exclusive shared access credential.

Procedure

1. Copy the App ID Toolkit (`ibmappid.jar`) to a directory on the computer. For example: `C:\IBM\ibmappid.jar`
2. Register the script. See “Registering an Application Instance” on page 180. Ensure that the application type is set to 2 (Script).

The fingerprint of a script does not include information about the contents or the file location of the script.

Any script that is running as the same user in the same computer will be regarded by the fingerprinting function as the same instance.

If you want to separate one script from another, specify a group name (`-g`) when you register the script. The same group name must be specified in Step 4 to retrieve credentials.

For example: `java -jar C:\IBM\ibmappid.jar register-first-instance -s pim.example.org -a SSHClient -n SSHClient@MaintServer -t 2 -g ssh-scripts`

Note: The implementation of fingerprinting and the definition of an application instance for licensing purposes are independent of each other. Entitlements must be purchased for any distinct script of an application that is managed by the program.

3. Grant the script access to the credential that it needs. See “Granting an application access to shared credentials on resources” on page 182. For example: Entitle the application `SSH Client` to the credential, `remote1` in the service `unixsvr01.example.org`.

4. Run the App ID Command Line Tool in silent mode to verify that the script is able to get the credentials: `java -jar C:\IBM\ibmappid.jar get-credential -s <PIM VA URL> -n <App Instance Name> -r <Resource Alias> -g <Group Name> -x` For example: `java -jar C:\IBM\ibmappid.jar get-credential -s pim.example.org -n SSHClient@MaintServer -r unixsvr01.example.org -g ssh-scripts -x`

If the command is successful, the tool exits with code 0 and you will see the retrieved user name and password, which is separated by a new line. For example:

```
remotel
s3crEt
```

If the tool encounters an error, the tool exits with a nonzero code and you see an error message. For example: CTGSAE018E There are no credential entitlements that can be used.

5. Modify the script to get credentials from IBM Security Privileged Identity Manager.

- a. Identify the code in the script, which contains hardcoded credentials.

```
...
# Example Perl script
my $username="remotel";
my $password="s3crEt";

$ssh->login($username, $password);
...
```

- b. Add a statement to run the App ID Command Line Tool from the script. Use the command that you validated in Step 4.

```
...
my $output=`java -jar C:\IBM\ibmappid.jar get-credential -s pim.example.org
-n SSHClient@MaintServer -r unixsvr01.example.org -g ssh-scripts -x`;
...
```

- c. Add a statement to check the exit code of the command. If the command exits successfully, parse the output, and use the credentials.

```
...
if ($? == 0) {
my @credentials=split(/\n/, $output);
$ssh->login($credentials[0], $credentials[1]);
} else {
print('Failed: ' + $output);
}
...
```

Providing managed credentials to data source connections for WebSphere Application Server applications

You can configure the WebSphere Application Server to use the App ID Java EE data source for establishing database connections by using managed credentials from the IBM Security Privileged Identity Manager.

Before you begin

Refer to the Software Product Compatibility Report to ensure that the App ID Toolkit supports the WebSphere Application Server server version and the database that you use.

For WebSphere Application Server in a cluster, repeat the following steps on each node.

Add the database credential as a non-exclusive shared credential.

Procedure

1. Copy the App ID Toolkit (`ibmappid.jar`) to a directory on the computer. For example: `C:\IBM\ibmappid.jar`
2. Register the script. See “Registering an Application Instance” on page 180. Ensure that the application type is set to 3 (Data source).
For example: `java -jar C:\IBM\ibmappid.jar register-first-instance -s pim.jke.org -a TestApp -n TestApp@server1 -t 3 -g test-apps`

Important:

- You must use the same Java Runtime Environment as used by your application server to run the App ID Toolkit during registration. For example: `run C:\IBM\WebSphere\AppServer\java\bin\java.exe -jar ibmappid.jar`
 - If WebSphere Application Server runs under Local System account in Windows, specify the operating system user as `"nt authority\system"` during registration (`-o "nt authority\system"` or `--os-user "nt authority\system"`).
3. Create a WebSphere variable to point to the folder where you place the App ID Toolkit. For example: `APPID_JDBC_DRIVER_PATH=${WAS_INSTALL_ROOT}/appid`
 4. Create a JDBC provider.

Note: For a clustered deployments, before you create a JDBC provider and the data source, under **Scope**, select the node from the list.

- a. Select **Resources > JDBC > JDBC providers**.
- b. Set the database type to **User-defined**.
- c. The connection pool implementation class name is `com.ibm.ispim.appid.jdbc.AppIdConnectionPoolDataSource`.
- d. Assign a JDBC provider name. For example: `AppID JDBC Provider`.
- e. Specify the class path information. Provide the path to locate `'ibmappid.jar'`.

Note: For clustered deployments, for JDBC Provider, give the location of the `ibmappid.jar` in the node's host machine.

For example: `${APPID_JDBC_DRIVER_PATH}/ibmappid.jar`

- f. After the JDBC provider is created, open the configuration page and select the **Isolate this resource provider** check box.
5. Note the JNDI key of the existing connection pooled data source for your application. For example: `jdbc/testapp`
 6. Replace the JNDI key of the existing connection pooled data source with another value. For example: `jdbc/testappdirect`
 7. Create the data source.
 - a. Assign a data source name. For example: `Appid testapp datasource`.
 - b. Specify the JNDI key noted in step 5.
 - c. Use the JDBC provider that you created in step 6.
 - d. Save the information.

- e. Under **Additional Properties**, click **WebSphere Application Server data source properties** and set **Set Statement Cache size** to 0 to disable statement caching.
- f. Specify the following custom properties:

Table 19. Custom Properties

Name	Value	Example
url	The PIM VA URL and original data source JNDI name, in the format of: jdbc:appid://<PIM VA URL>/dsjndi=<name from Step 6>	jdbc:appid://pim.jke.org/dsjndi=jdbc/testappdirect
appinstance	Registered Application Instance name.	TestApp@server1
workspace	Workspace specified during registration. If you used the default workspace, specify the folder containing ibmappid.jar.	C:\Program Files\IBM\WebSphere\AppServer\appid
serviceurl	Resource URI or alias of the managed credential to be retrieved.	proddb.jke.org
username	Optional: User name of the managed credential to be retrieved. Useful when there are multiple credential entitlements for one resource.	db2inst1
group	Optional: Application Instance group ID, if specified during registration.	test-apps

- 8. Do a **Test Connection** on the newly created data source.

Providing managed credentials to a Java application

You can modify Java applications to use the App ID Java SDK to retrieve managed credentials from the IBM Security Privileged Identity Manager Server.

Before you begin

- Refer to the Software Product Compatibility Report to ensure that the App ID Toolkit supports the Java Runtime Environment that your application uses.
- Review the App ID Java SDK documentation in App ID Java API
- Add the application credential as a non-exclusive shared credential.

Procedure

1. Import the App ID Toolkit (ibmappid.jar) to your development environment and include it in your build path.
2. Modify the application code to get credentials from IBM Security Privileged Identity Manager.
 - a. Identify the code that uses the credentials.

```

...
// Example Java code that reads credentials from a properties file
String username = prop.getProperty("user");
String password = prop.getProperty("pass");
connect(username, password);
...

```

- b. Create an instance of AppIDManager, specifying the application instance name and the IBM Security Privileged Identity Manager virtual appliance URL. If you want to specify a group ID or use a specific token store folder, you can specify them here as well.

```

...
try {
    //com.ibm.ispim.appid.client.api.AppIDManager
    AppIDManager appIDManager = AppIDManager.create()
        .withAppInstanceName("hrapp_instance1")
        .withServerURL(new URL("https://pimva.jke.org"))
        .withWorkspace ("C:\\AppID Workspace")
        .withGroupName("group1") //optional
        .withOAuthTokenFolder("C:\\IBM\\ISPIM\\tokens") //optional
        .build();
} catch (ExecutionException e) {
    logger.error(e.getMessage());
}
...

```

- c. Retrieve the managed credentials using `getCredential` method.

```

...
//com.ibm.ispim.appid.client.api.Credential
Credential ldapCred;

try {
    ldapCred = appIDManager.getCredential("ldap.jke.org")
} catch (ExecutionException e) {
    logger.error(e.getMessage());
}
...

```

- d. Use the username and password contained in the retrieved `Credential` object.

```

...
String username = ldapCred.getUserID();
String password = ldapCred.getPassword();
connect(username, password);
...

```

- e. Compile and deploy the application.

3. Register the Java application using the steps for “Registering an Application Instance.”

Ensure that the application type is set to 1 (Java Application) and that you use the same group name and token store path as specified in the application code.

During registration, provide the following information:

- Binary class name (`-l` or `--class-name`): The fully qualified name of the class that invokes `getCredential()`. For example: `org.jke.hrapp`
- Path to the JAR file (`-b` or `--binary-path`): The path to the JAR file that contains the class that invokes `getCredential()`. For example: `C:\JKE\HRApp\bin\hrapp.jar`

The fingerprint of a Java application includes its binary hash and path. You should only perform the registration after making the changes to the application code and putting the application JAR file in its final location.

Application identity management tasks

The tasks for managing application identities include registering the application instance, setting up the credentials to be used by the application, and setting up the entitlements for an application.

Registering an Application Instance

A domain administrator can register application instances into the administrative domain. The registration process collects the fingerprint of the application instance and grants an OAuth 2.0 token for the instance.

About this task

Application instances are registered by running the command line tool in the App ID Toolkit (`ibmappid.jar`) on the computer where the application or script runs.

The command line tool provides two commands for Application Instance registration:

- **register-first-instance**: Register a new application and the first instance.
- **register-additional-instance**: Add an instance to an application that already exists in the user's administrative domain.

Note: To register an instance of a registered application without any instances, use the `register-additional-instance` command. For example, use the **register-additional-instance** command. If you have previously registered HRApp application with an instance `hrapp_1`, and subsequently deleted `hrapp_1`, leaving HRApp without any instance.

Procedure

1. Run the **register-first-instance** or **register-additional-instance** command:
java -jar ibmappid.jar register-first-instance.
2. Provide the following information when prompted:

Prompt	Equivalent switch	Expected input
Enter your user name:	-u --user-name	PIM domain administrator user name
Enter your password:	-p --password	PIM domain administrator password
Enter path of the workplace folder:	-w --workspace	Path of the workspace to store SSL certificates and tokens, default: parent folder of <code>ibmappid.jar</code>
Enter server URL:	-s --server	URL of the IBM Security Privileged Identity Manager Server
Enter application type (1=Java, 2=script, 3=data source):	-t --application-type	Type of the application
Enter application name:	-a --application-name	Name of the application
Enter application instance name:	-n --instance-name	Name of the application instance
Enter application instance description:	-d --instance-description	Description of the application instance, default: empty
Enter group ID:	-g --group-id	Group name for separating two application instances that have the same fingerprint, default: empty

Prompt	Equivalent switch	Expected input
Enter the operating system user who will run the application:	-o --os-user	Operating system user name, the application instance will run under this user name, default: current user If you are registering an instance for a different user, for example, a user who belongs to a domain, the value you provide for "Enter the operating system user who will run the application instance" during instance registration must match the output of the whoami command for that user. For example, consider you are registering an instance for a user User1 who is part of domain test.example.com. Run whoami while logged in as User1. If whoami returns test\user1, this is the value you must use for the operating system user.
Enter resource UID or alias:	-r --resource-uid	Resource UID or alias to use, for which credential should be check out.
Enter user name to be retrieved:	-c --credential-username	User name of the credential to be retrieved, default: empty (any credential will be accepted)
Enter binary path	-b --binary-path	Path of the JAR file containing the class that uses AppIDManager
Enter class name	-l --class-name	Full name of the class using AppIDManager

The process completes successfully with this message: (Application instance name) created successfully.

If you are registering the first instance of an application, use the Service Center to grant the application access to a set of credentials or credential pools. See "Granting an application access to shared credentials on resources."

Granting an application access to shared credentials on resources


As an application administrator, after you register the first application instance, grant the application the right to use a set of shared credentials or credential pools on resources.

Before you begin

- Authorize the first instance of an application.
- Add the resource.
- Add credentials for the resource.

Procedure

1. Log on to service center at <https://<PIM VA URL>/ispim/ui/>.
2. Click **Manage Applications**.
3. Select the registered application instance. For example: DemoApp

4. Click **Manage Entitlements**  .
5. On the **Entitlements** page, browse for the credentials that the application can access.
6. Click **Add** to specify the credential entitlements that you want to grant to the application.
7. Click **Submit**.

Managing the list of authorized applications

Use the **Manage Applications** page in the Privileged Identity Manager Service Center to browse, search, and delete the authorized application instances.

Before you begin

- You are a member of the Privileged Administrator group.
- You are a domain administrator.


Procedure

1. Log on to the Privileged Identity Manager Service Center.
2. Click **Manage Applications**.
3. You can perform the following tasks:


Search for an application

Use the search input box on top of the application list to search for an application by its name.


Edit the name of an application

Select an application and click the pencil icon  next to its name to edit the application name.


Delete an application

Select an application and click the minus icon  next to its name to delete the application and all of its instances. The application will be removed from all shared access policies that it is currently entitled to. If any shared access policy has no member after this, the policy will be removed.


Edit the description of an application instance

Select an application, then select the instance. Click pencil icon  next to the instance name to edit the application instance description.


Delete an application instance

Select an application, then select the instance. Click the minus icon  next to the instance name to delete the application instance.


Suspend an application instance

Select an application, then select the instance. Click the suspend icon  next to the instance name to suspend the application instance. The application instance will not be able to get managed credentials when it is suspended.


Restore a suspended application instance

Select an application, then select the instance. A suspended instance will have a `SUSPENDED` indication below its description. Click the restore icon  next to the instance name to restore the application instance.

Edit the fingerprint matching policy of an application instance

Select an application, then select the instance. Click the pencil icon  next to the instance name and select the policy from the selection box. For a description of the policies, see “Application instance fingerprint” on page 174.

Manage entitlements for an application

Select an application. Click the entitlements icon  next to the instance name and define the credential entitlements for the application.

Chapter 15. Report administration

The IBM Security Privileged Identity Manager solution supports the IBM Cognos® reporting framework for report generation.

Available reports

The reporting package includes the following reports:

Application ID Registration Report

This report shows the registered application instances and the details about each registered instance such as the host, instance name, and description.

Application Instance Activity Audit Report

This report shows the auditable events or actions that have occurred with privileged credentials on a registered application instance.

Shared Access Entitlements by Owner Report

This report shows the credentials and credential pools that are owned by the selected owner.

Shared Access Entitlements by Role Report

This report shows the information about the credentials and credential pools that are entitled by the selected role.

Shared Access Entitlement Definition Report

This report shows the configuration information of Privileged IDs and the Shared Access Policies that are associated with these Privileged IDs.

Shared Access History Report

This report shows the history of actions that are performed on the shared credentials.

Single Sign-On Privileged ID Audit Report

This report provides a log history of check-out and check-in actions that are performed for each Privileged ID on the managed resource. This report also includes a subreport that is called User Activity Audit Report. With this subreport, you can play back the user session recording or view the terminal commands that the user executed on the managed resource.

Privileged Session Recorder Report

This report shows the history of activities that occurred in the Privileged Session Recorder console. You can use this report to track and monitor the actions of the selected user in the Privileged Session Recorder console.

For more information about these reports, see “Report descriptions and parameters” on page 188.

Note: For the shared access reports, you must map the attributes to the entities before you can work with these reports. For more information about mapping the attributes, see “Mapping the attributes and entities” on page 204.

Report data overview

Report data is staged through a data synchronization process. The process gathers data from the directory information store and prepares it for the reporting engine. You can run data synchronization on demand or schedule it on a regular basis.

The generated reports are based on the most recent data synchronization, not on current data. Activities that occur after the last completed data synchronization are captured by the next data synchronization. Data in the reports is obtained from the database and the directory server.

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.

For more information, see “Data synchronization” on page 195.

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.

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 20. Basic tasks to configure report model

Tasks	Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp
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 .

Scenarios

See the possible scenarios that can be used to customize the IBM Security Privileged Identity Manager Cognos report model.

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 `<data_source>` database schema. For example: ISPIM.
 - a. In the IBM Security Privileged Identity Manager administrative console, select **Configure System > 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 **Configure System > Data Synchronization**.
 - b. Click **Run Synchronization Now**.
3. Add the information about email address in the reporting package **ISPIMReportingPackage_2.0.1**.
 - a. Open the Framework Manager.
 - b. Select the report project **ISPIMReportingPackage_2.0.1**.
 - c. Right click and select **Run Metadata Wizard**.
 - d. From the Metadata Wizard window, select **Data Source** and click **Next**.
 - e. Select `<data_source>` and click **Next**. You must use the data source name **ISPIM**.
 - f. Select the ITIMUSER object and click **Tables**.
 - g. Select the PERSON_MAIL table and click **Next**.
 - h. Clear the **Use primary and foreign keys** check box.
 - i. Click **Import**.
 - j. 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.

Report descriptions and parameters

Each of the Privileged Identity Manager Cognos-based reports have parameters, which you can use to filter the scope of the report.

To create and view these reports, see “Generating the report through IBM Cognos Business Intelligence” on page 225.

Note:

- You must map the attributes to the entities before you work with the IBM Cognos shared access reports. For more information about mapping the attributes, see “Mapping the attributes and entities” on page 204.
- You must set the locale to English or to any supported language before you run any of the reports. See Setting language preferences. 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.

Application ID Registration Report

This report shows the registered application instances and the details about each registered instance such as the host, instance name, and description.

Table 21. Filters for the Application ID Registration Report

Parameter	Description
Application Name	The name of the application.
Application Business Unit	The name of the business unit.
Application Instance	The name of the application instance.
Registered By	The name of the user who registers the application instance.
Host Name	The host name of the system where the application instance is located.

Application Instance Activity Audit Report

This report shows the auditable events or actions that have occurred with privileged credentials on a registered application instance.

Table 22. Filters for the Application Instance Activity Audit Report

Parameter	Description
Application Name	The name of the application.
Business Unit	The name of the business unit.
Application Instance	The name of the application instance.
Registered By	The name of the user who registers the application instance.
Audit Event	Displays the action that is performed on the shared access credential. The supported audit events are Check-out and Check-in.

Shared Access Entitlement by Owner Report

This report shows the credentials and credential pools that are owned by the selected owner.

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 23. Filters for Shared Access Entitlement by Owner Report

Parameter	Description
Entitlement Type	Displays the type of an entitlement, such as credential or credential pool.
Credential Service Business Unit	Displays the business unit that is associated with the credential service.
Credential Service	Displays the service information that has the credential entitlements that are associated with it.
Credential Owner	Displays the shared access owner.
Credential	Displays the shared access.
Credential Pool Service Business Unit	Displays the business unit that is associated with the shared access pool service.
Credential Pool Service	Displays the service information that has the shared access pool entitlements that are associated with it.
Credential Pool Owner Type	Displays the shared access pool owner type.
Credential Pool Owner	Displays the shared access pool owner.
Credential Pool	Displays the shared access.

See “Generating the report through IBM Cognos Business Intelligence” on page 225.

Shared Access Entitlement by Role Report

This report shows the information about the credentials and credential pools that are entitled by the selected role.

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 24. Filters for Shared Access Entitlement by Role Report

Parameter	Description
Role Business Unit	Displays name of the business unit of the role.
Role	Displays the list of roles.
Entitlement Type	Displays the type of an entitlement, such as credential or credential pool.

See “Generating the report through IBM Cognos Business Intelligence” on page 225.

Shared Access Entitlement Definition Report

This report shows the configuration information of Privileged IDs and the Shared Access Policies that are associated with these Privileged IDs.

The following table describes the parameters for filtering the report.

Table 25. Filters for the Shared Access Entitlement Definition Report

Parameter	Description
Business Unit	Displays the business unit that is associated with the shared access credential service.
Service	Displays the service of the Privileged ID.
Credential Owner	Displays the name of the Privileged ID owner.
Credential Name	Displays all the credentials that are associated to the Shared Access Policies.
Credential Pool Name	Displays all credential pools that are associated to the Shared Access Policies.

See “Generating the report through IBM Cognos Business Intelligence” on page 225.

Shared Access History Report

This report shows the history of actions that are performed on the shared credentials.

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 26. Filters for Shared Access History Report

Parameter	Description
Audit of	Displays the entitlement types for which an audit is performed. For example, credential, or credential pool.
Start Date	Displays the start date of the shared access history.
End Date	Displays the end date of the shared access history.
Service Business Unit	Displays the business unit that is associated with the service.
Service	Displays the service information that has the shared access that is associated with it.
Credential Owner	Displays the shared access owner name.
Credential	Displays the shared access.
Credential Pool Owner Type	Displays the type of the shared access owner. The type of owner can be either a person or a role.
Credential Pool Owner	Displays the shared access owner name. The owner name can be either a person name or a role name.
Credential Pool	Displays the shared access pool.

See “Generating the report through IBM Cognos Business Intelligence” on page 225.

Single Sign-On Privileged ID Audit Report

This report provides a log history of check-out and check-in actions that are performed for each Privileged ID on the managed resource. This report also includes a subreport that is called User Activity Audit Report. With this subreport, you can play back the user session recording or view the terminal commands that the user executed on the managed resource.

You can use the Single Sign-On Privileged ID Audit Report to audit all automated check-out and check-in of shared access credentials from the IBM Security Privileged Identity Manager server through IBM Security Access Manager for Enterprise Single Sign-On.

The following table describes the parameters for filtering the report.

Table 27. Filters for the Single Sign-On Privileged ID Audit Report

Parameter	Description
Audit Operation Date Range: Start Date	Displays all events from the specified date.
Audit Operation Date Range: End Date	Displays all events until the specified date.
User Name	Displays the Privileged user whose operation needs to be audited.
User Machine IP Address	Displays the unique identifier of the machine that is used by the IBM Security Access Manager for Enterprise Single Sign-On user.
Privileged ID	Displays the shared access credential.
Audit Event	Displays the action that is performed on the shared access credential. The supported audit events are Check-out and Check-in.
Managed Resource	Displays the unique identifier of the managed resource.

See “Generating the report through IBM Cognos Business Intelligence” on page 225.

User Activity Audit Report

To view the activity details of a user on a selected managed resource, click the corresponding **Click to view** link in **User Activity**. The User Activity Audit Report is displayed in a new window. This report contains a Recorded Sessions and a Recorded Terminal Commands section.

To watch the recording of the user session on the managed resource, click the Session Recording Link. To enable this feature, see Enabling session recording replay from the report.

Privileged Session Recorder Report

This report shows the history of activities that occurred in the Privileged Session Recorder console. You can use this report to track and monitor the actions of the selected user in the Privileged Session Recorder console.

You can determine from which computer the user accessed the console. You can also determine the status of the actions.

The following table describes the parameters for filtering the report.

Table 28. Filters for the Privileged Session Recorder Report

Parameter	Description
Audit Operation Date Range: Start Date	Displays all events from the specified date.
Audit Operation Date Range: End Date	Displays all events until the specified date.
User Name	Displays the Privileged user whose operation needs to be audited.
Server Address	Specifies the target server host name or IP address location where the user is logged on.
Client Machine IP Address	Specifies the client address location.

See “Generating the report through IBM Cognos Business Intelligence” on page 225.

Report models

Use the IBM Security Privileged Identity Manager Cognos report models to generate different types of reports that suit your requirements.

IBM Cognos report models consists of the following objects.

Query Items

Query items are the smallest pieces 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

Query subjects consists of 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.

Namespaces

Uniquely identifies query items, dimensions, query subjects, and other objects. You import different databases into separate namespaces to avoid duplicate names.

Packages

Creates reports, analyses, and ad hoc queries. Packages are 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.

Single Sign-On Module model

You can use the Single Sign-On Module model to customize the Single Sign-On Privileged ID Audit Report.

The Single Sign-On Module model for IBM Security Privileged Identity Manager consists of the following namespaces:

Table 29. Single Sign-On Module model namespaces

Namespace	For information about query subjects and query items, see
Single Sign-On Audit	"Single Sign-On Audit namespace for Single Sign-On Module" on page 205.
PSR Audit	"PSR Audit namespace for Single Sign-On Module" on page 207

Shared Access Management model

You can use the Shared Access Management model to customize the shared access reports.

The Shared Access Management model consists of two namespaces:

Table 30. Shared Access Management model namespaces

Namespace	For information about query subjects and query items, see
Audit	"Audit namespace for shared access module" on page 208.
Configuration	"Configuration namespace for shared access module" on page 213.

Application ID Module model

You can use the Application ID Module model to customize the Application ID Registration Report.

The Application ID Module model for IBM Security Privileged Identity Manager consists of the following namespace:

Table 31. Application ID Module model namespaces

Namespace	For information about query subjects and query items, see
Application ID Configuration	"Application ID Configuration namespace for Application ID Module" on page 221.
Application Instance Activity Audit	"Application Instance Activity Audit namespace for Application ID Module" on page 223

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.

Note: Map only the entities and attributes for which you want to generate custom reports. These mappings directly affect the performance of IBM Security Privileged 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 Privileged 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.

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.

Procedure

1. Click **Configure System > 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.

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.

Procedure

1. Click **Configure System > 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**.

Data synchronization

IBM Security Privileged 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 Privileged Identity Manager, the policies that are defined in IBM Security Privileged Identity Manager, and other information.

IBM Security Privileged 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 Privileged 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 Privileged Identity Manager, and run the full data synchronization process.

On a recurring schedule

As an administrator, you can configure IBM Security Privileged Identity Manager to automatically run the full data synchronization process on a specified recurring schedule. For example, you can configure IBM Security Privileged 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 Privileged Identity Manager environment. That is, the first two approaches must be run on a computer in which IBM Security Privileged 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.

Procedure

1. Click **Configure System > 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.

Procedure

1. Click **Configure System > 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

A data synchronization schedule must exist.

Procedure

1. Click **Configure System > 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

A data synchronization schedule must exist.

Procedure

1. Click **Configure System > 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 Privileged Identity Manager uses and the IBM Security Privileged 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 Privileged 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 Privileged 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 Privileged 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 Privileged Identity Manager, see the appropriate documentation provided by the vendor of that directory server.

Note: Enabling the IBM Security Privileged 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.

Table 32. Definitions for directory variables

Path Abbreviation	Description
ISPIM_HOME	INSTALL_DIR/ISPIM INSTALL_DIR is the location of the IBM Security Privileged 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 Privileged Identity Manager Server and synchronize the data with the Synchronize Data task in the IBM Security Privileged Identity Manager console *before* you start the Incremental Data Synchronizer.

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

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 Express/IBM Security Privileged 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

Install the Incremental Data Synchronizer.

See the topic "Installing the Incremental Data Synchronizer" in the chapter "Optional post-installation tasks" in the *IBM Security Identity Manager Installation Guide*.

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:

Table 33. Parameters and arguments for the Incremental Data Synchronizer script

Argument	Description
<i>itim-manager</i>	Login ID of IBM Security Identity Manager Express IBM Security Privileged Identity Manager system administrator
<i>passwd</i>	Password for login ID
<i>chglog-base-dn</i>	Base DN of Security Identity Manager Express IBM Security Privileged Identity Manager directory server <i>changelog</i> entries, for example, <code>cn=changelog</code>
<i>time-int</i>	Time interval between successive synchronizations
<i>runInBackground</i>	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 Privileged 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 Privileged 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 WebSphere Application Server, a directory server, or a database.

The utility for external report data synchronization is used for remote or non-IBM Security Privileged Identity Manager purposes. The IBM Security Privileged 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 `ISPIM_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 Privileged Identity Manager report data synchronization utility.
- Access the folder in which you extracted the utility.

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 34 for specifying the location of the Java runtime environment.

Table 34. Specifying the location of the Java runtime environment

If the <code>-JAVA_HOME</code> argument is	IBM Security Privileged Identity Manager
• Specified	Uses the corresponding Java runtime environment.

Table 34. Specifying the location of the Java runtime environment (continued)

If the <code>-JAVA_HOME</code> argument is	IBM Security Privileged Identity Manager
<ul style="list-style-type: none"> • Not specified, and • The <code>-JAVA_HOME</code> operating system environment variable contains a value. 	Uses the Java runtime environment corresponding to the <code>-JAVA_HOME</code> operating system environment variable.
<ul style="list-style-type: none"> • Not specified, and • The <code>-JAVA_HOME</code> 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.

Query subjects and query items for the report models

Use the query subjects and query items information to customize the Privileged Identity Manager Cognos-based reports.

Mapping the attributes and entities

You must map the attributes to the entities before you can work with the query items for the IBM Cognos shared access report and Application ID Registration Report models.

After you map the schema by using the IBM Security Privileged Identity Manager administration console, you must

- Run a successful data synchronization.
- Restart the IBM Cognos Business Intelligence Server version 10.2.1 Fix Pack 1 to reflect the updated schema in the report.

The IBM Cognos report does not reflect the updated data immediately.

Table 35. Mapping the attributes and entities

Namespace	Entity	Attribute Name
Application ID Configuration	AppInstance	<ul style="list-style-type: none"> • Application Instance Description (erpappinstancedescription) • Application Instance Fingerprint (erpappinstancefingerprint) • Application Instance Name (erpappinstancename) • Application Instance Registrant Name (erpappinstanceregistrant) • Application Instance Type (erpappinstancetype) • Parent DN
	Person	<ul style="list-style-type: none"> • First name • Full name • Last name • Organizational roles • Parent DN • Status • Supervisor
	Static Role	<ul style="list-style-type: none"> • Classification • Description • Name • Parent DN
Application Instance Activity Audit	AppInstance	<ul style="list-style-type: none"> • Application Instance Description (erpappinstancedescription) • Application Instance Fingerprint (erpappinstancefingerprint) • Application Instance Name (erpappinstancename) • Application Instance Registrant Name (erpappinstanceregistrant) • Application Instance Type (erpappinstancetype) • Parent DN
	Person	<ul style="list-style-type: none"> • First name • Full name • Last name • Organizational roles • Parent DN • Status • Supervisor
	Static Role	<ul style="list-style-type: none"> • Classification • Description • Name • Parent DN

Single Sign-On Audit namespace for Single Sign-On Module

The Single Sign-On Audit namespace provides information about the history of actions for the Privileged ID.

Query subjects for Single Sign-On Audit namespace

The following table lists the query subjects in the Single Sign-On Audit namespace for the Single Sign-On Module model.

Table 36. Query subjects in the Single Sign-On Audit namespace

Query subject	Description
Checkout Checkin Audit	Represents the audit of actions that are performed on the Privileged ID. This query subject can generate an audit report for these actions: Check-out, and Check-in.
User Activity Audit	Represents the audit of actions that are performed by the user on the managed resource. This query subject can generate an audit report for the recorded sessions and terminal commands that the user executed.

Query items for Single Sign-On Audit namespace

The following table lists the query items in the Single Sign-On Audit namespace.

Table 37. Query items in the Single Sign-On Audit namespace

Query subject	Query items and their description
Checkout Checkin Audit	<p>User Name The unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user.</p> <p>Authentication Service The users authentication service that is defined in IBM Security Access Manager for Enterprise Single Sign-On.</p> <p>Application User ID User who has the privileges to check-out and check-in the shared access credential.</p> <p>Audit Event The action that is performed on the shared access credential. The supported audit events are Check-out and Check-in.</p> <p>Event Code The numeric code assigned for the audit event.</p> <p>Result Indicates whether the Audit Event is successful or not.</p> <p>User Machine IP Address The user computer IP address.</p> <p>User Machine Host Name The user machine host name.</p> <p>Server The server machine IP address or host name.</p> <p>Timestamp The time when the Audit Event happened.</p> <p>Managed Resource The IP address or host name of the Managed Resource.</p> <p>Credential Pool The name of the credential pool from which the Privileged ID is retrieved.</p> <p>Privileged ID The shared access credential privileged identity.</p> <p>Application The name of the application that the user accessed with a Privileged ID.</p> <p>Session Recording ID The unique identifier for the session recording link.</p>

Table 37. Query items in the Single Sign-On Audit namespace (continued)

Query subject	Query items and their description
User Activity Audit	<p>Recording ID The unique identifier for the session recording link.</p> <p>Bookmark ID The unique identifier that is a reference to a frame in the recording. It is a frame where a command is recognized.</p> <p>Frame Sequence Number The unique sequence number of a frame where a command is entered.</p> <p>Type The bookmark type. For instance, a command bookmark in a text-based recording is of type 1.</p> <p>User ID The Unique identifier of Privileged Identity Manager User.</p> <p>Privileged ID The shared access credential privileged identity.</p> <p>Command Executed The terminal command executed on the managed resource using PUTTY application by the Privileged Identity manager user.</p> <p>Command Execution Time The Date and time when the Privileged Identity Manager user has executed the terminal commands on managed resource using PUTTY application.</p> <p>Local User ID The Windows user who logged on a client computer.</p> <p>Application Name Application used by the Privileged Identity Manager user to perform activity on managed resource. For instance : PUTTY, RDP, and PCOMM.</p> <p>Local Host The host name of local machine.</p> <p>Managed Resource The IP address or host name of the Managed Resource.</p> <p>Recording Start Time The start date and time when the recording has begun.</p> <p>Recording End Time The end date and time when the recording has completed.</p>

PSR Audit namespace for Single Sign-On Module

The PSR Audit namespace provides information about the history of all session recording actions performed by the User.

Query subjects for PSR Audit namespace

The following table lists the query subjects in the PSR Audit namespace for the PSR Audit model.

Table 38. Query subjects in the PSR Audit namespace

Query subject	Description
PSR Audit Event	Represents the audit of actions that are performed on the users session recordings.

Query items for PSR Audit namespace

The following table lists the query items in the PSR Audit namespace.

Table 39. Query items in the PSR Audit namespace

Query subject	Query items and their description
PSR Audit Event	<p>Audit ID The unique ID for the session recording activity audit record.</p> <p>Event ID The numeric code assigned for the audit event.</p> <p>User Name The unique identifier of the IBM Security Access Manager for Enterprise Single Sign-On user.</p> <p>Event Time The time when the Audit Event happened.</p> <p>Result Indicates whether the Audit Event is successful or not.</p> <p>Event Details Provides description of the session recording event.</p> <p>Server Address The server machine IP address or host name.</p> <p>Client Address Specifies the client address location.</p>

Audit namespace for shared access module

The Audit namespace provides information about the history of actions for the shared access.

Query subjects for Audit namespace

The following table lists the query subjects in the Audit namespace for the shared access module model.

Table 40. Query subjects in the Audit namespace

Query subject	Description
Shared Access Audit	Represents the audit of actions that are performed on the shared credentials. This query subject can generate an audit report for these actions: Checkout, Checkin, ViewPassword, NotifyExpiredLease, and NotifyCheckinExpiredLease.
Account	Represents account and its configuration attributes. You must use this query subject with the Credential to obtain information about the account that is associated with a credential.
Account Owner	Represents a user owner of an account that is associated to the shared credential. You must use this query subject with the Account to obtain information about user owner of the account.
Credential	Represents a credential on which the audit action is performed. You must use this query subject with the Shared Access Audit to obtain information about a credential and its configuration attributes.
Credential Service	Represents the service on which an account associated with the credential is provisioned. You must use this query subject with the Account to obtain information about the service and its configuration attributes.
Credential Service Business Unit	Represents a business unit that is associated to the credential service. You must use this query subject with the Credential Service to obtain information about the configuration attributes of the business unit.

Table 40. Query subjects in the Audit namespace (continued)

Query subject	Description
Credential Pool	Represents a pool of credentials on which the audit action is performed. You must use this query subject with the Shared Access Audit to obtain information about the credential pool and its configuration attributes.
Credential Pool Owner	Represents an owner of the pool of credentials on which the audit action is performed. You must use this query subject with the Credential Pool to obtain information about a user or a role owner of the credential pool and its configuration attributes.
Credential Pool Business Unit	Represents a business unit that is associated with the credential pool. You must use this query subject with the Credential Pool to obtain information about the configuration attributes of the business unit.

Query items for Audit namespace

The following table lists the query items in the Audit namespace.

Table 41. Query items in the Audit namespace

Query subject	Query items and their description
Shared Access Audit	<p>Audit Action The action that is performed by a user on the credential. The valid values are Checkout, NotifyExpiredLease, ViewPassword, Checkin, and NotifyCheckinExpiredLease.</p> <p>Audit Date The date and time of the audit action.</p> <p>Audit Comments The comments that are specified by a user during audit action.</p> <p>Audit Justification The justification that is provided by a user during the check-out action.</p> <p>Audit Pool Name The name of the pool if a credential on which the audit action performed belongs to the credential pool.</p> <p>Audit Result Status The result of the audit action. The valid values are Success, Timeout, Warning, Failed, and In Progress.</p> <p>Audit Lease Expiration Time The check-out lease expiration time of a credential in time stamp form.</p> <p>Audit Credential Business Unit The name of a business unit to which an account corresponding to the credential belongs.</p> <p>Audit Initiator Name The name of a user who initiated the audit action on a credential.</p> <p>Audit Pool Dn The Lightweight Directory Access Protocol (LDAP) distinguished name for the audit pool.</p>

Table 41. Query items in the Audit namespace (continued)

Query subject	Query items and their description
Account	<p>Account Name The name of an account that is associated with a credential.</p> <p>Account Service Dn An LDAP distinguished name for a service that provisions an account.</p> <p>Account Status The detailed information of an account status.</p> <p>Account Compliance The details about an account compliance. The valid values are Unknown, Compliant, Non Compliant, and Disallowed.</p> <p>Account Ownership Type The ownership type of the account. The valid values are Individual, System, Device, and Vendor.</p> <p>Account Last Access Date The last accessed date and time of an account.</p> <p>Account Container Dn An LDAP distinguished name for a business unit of an account.</p>
Account Owner	<p>Full Name The full name of a user who owns an account.</p> <p>Last Name The surname of a user who owns an account.</p> <p>Type The profile type of the user, which is person.</p> <p>Status The status of a user who owns an account. Status is either Active or Inactive.</p> <p>Supervisor The supervisor of a user who owns an account.</p> <p>Business Unit Name The name of a business unit to which an account owner belongs.</p> <p>Dn An LDAP distinguished name for a user owner of an account corresponding to a credential.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit to which an account owner belongs.</p>

Table 41. Query items in the Audit namespace (continued)

Query subject	Query items and their description
<p>Credential</p>	<p>Credential Name The name of a credential on which the audit action is performed.</p> <p>Credential Description The detailed description of a credential that is specified by an administrator during the addition of an account into the vault.</p> <p>Credential IS Exclusive Indicates whether the credential is exclusive or not. You must check out an exclusive credential to view its password or other details.</p> <p>Credential USE Global Settings A flag that indicates whether a credential uses the shared access global settings. 0 represents Uses global settings, and 1 represents Does not use global settings.</p> <p>Credential IS Searchable Indicates whether a credential is searchable or not. 0 represents Credential can be searched, and 1 represents Credential cannot be searched.</p> <p>Credential IS Password Viewable Specifies whether a user can view the password on a credential. 0 represents password is viewable, and 1 represents password is not viewable.</p> <p>Credential IS Checkedout Provides the status of the credentials. Yes represents that the credential is checked out, and No represents that the credential is available in the credentials vault and not yet checked out.</p> <p>Credential Account Status The status of an account corresponding to a credential whether it is active or inactive. 0 represents Active, and 1 represents Inactive.</p> <p>Credential Reset password Indicates whether the password of a credential is regenerated on every check-in action. 0 represents Yes, and 1 represents No.</p> <p>Credential MAX Checkout Time The maximum allowed check-out duration for the credential in hours.</p> <p>Credential Dn An LDAP distinguished name for a credential.</p> <p>Credential Account Dn An LDAP distinguished name for an account that is associated with a credential.</p>
<p>Credential Service</p>	<p>Service Name The name of the service on which an account is provisioned.</p> <p>Service Type The profile type of the service.</p> <p>Service Dn An LDAP distinguished name for the service on which an account is provisioned.</p> <p>Service Business Unit Dn An LDAP distinguished name for a business unit to which the service belongs.</p>

Table 41. Query items in the Audit namespace (continued)

Query subject	Query items and their description
Credential Service Business Unit	<p>Business Unit Name The name of a business unit to which the credential service belongs.</p> <p>Business Unit Supervisor A user supervisor of the business unit.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit to which the credential service belongs.</p> <p>Business Unit Container Dn An LDAP distinguished name for a business unit that applies to the action initiator organization.</p>
Credential Pool	<p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p> <p>Credential Pool Name The name of the credential pool.</p> <p>Credential Pool Service Dn An LDAP distinguished name for the service to which a group associated with a credential pool is provisioned.</p> <p>Credential Pool Business Unit Dn An LDAP distinguished name for a business unit of the credential pool.</p> <p>Credential Pool Use Global Settings An operational attribute that might be empty in case of credential pool.</p> <p>Credential Pool Object Profile Name An operational attribute that might be empty in case of credential pool.</p>
Credential Pool Owner	<p>Credential Pool Owner Name The name of the credential pool owner.</p> <p>Credential Pool Owner Type The description of a credential pool owner that is specified by an administrator during the credential pool configuration.</p> <p>Credential Pool Owner Business Unit The name of the business unit to which the credential pool owner belongs.</p> <p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p> <p>Credential Pool Owner Dn An LDAP distinguished name for a user or a role owner of the credential pool.</p>
Credential Pool Business Unit	<p>Business Unit Name The name of a business unit to which the credential pool belongs.</p> <p>Business Unit Supervisor The supervisor of a user who owns the business unit.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit to which the credential pool belongs.</p> <p>Business Unit Container Dn An LDAP distinguished name for a business unit.</p>

Configuration namespace for shared access module

The Configuration namespace provides the configuration level information about shared access entitlements and its supporting data. Only enabled policies are shown in this namespace.

Query subjects for Configuration namespace

The following table lists the query subjects in the Configuration namespace.

Table 42. List of query subjects in the Configuration namespace

Query subject	Description
Shared Access Policy Organization	Represents the business unit to which the shared access policy applies. You must use this query subject with the Shared Access Policy query subject. By doing so, you can obtain the configuration information about the business unit to which the shared access policy applies.
Shared Access Policy	Represents the shared access policy that provides entitlements for credentials and credential pools to a user or the role members. You must use this query subject with the Credential Entitled to Shared Access Policy and Credential Pool Entitled to Shared Access Policy.
Credential Entitled to Shared Access Policy	Represents the credentials that are entitled by using a shared access policy.
Credential Service	Represents the service on which a credential account is provisioned. You must use this query subject with the Account query subject to obtain configuration information about the account service.
Credential Service Organization	Represents the business unit of the credential service. You must use this query subject with the Credential Service query subject to obtain configuration information for the business unit of the service.
Role Owning Credentials	Represents the roles that have entitlements for credentials through a shared access policy. You must use this query subject with the Credential Entitled to Shared Access Policy to obtain information about the direct and indirect roles that have entitlements.
Credential Pool Membership	Represents the list of credential pool members. You must use this query subject with the Credential Entitled To Shared Access Policy query subject to obtain all credentials and the pools to which it belongs.
Account	Represents an account entity and some of its configuration attributes. You must use this query subject with the Credential Entitled to Shared Access Policy query subject to obtain information about: <ul style="list-style-type: none"> • The accounts that are configured as shared credentials. • The accounts that are entitled through the shared access policy.
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 account owners.
Credential Pool Entitled to Shared Access Policy	Represents the credential pools that are entitled by using a shared access policy.
Credential Pool Members	Represents the list of credential pool members. You must use this query subject with the Credential Pool Entitled To Shared Access Policy query subject to get all credentials and the pools to which it belongs.
Credential Pool Service Organization	Represents the business unit of the credential pool service. You must use this query subject with the Credential Pool Service query subject to obtain the configuration information about the service business unit.
Credential Pool Service	Represents the service on which the group corresponding to a credential pool is provisioned. You must use this query subject with the Credential Pool Entitled to Shared Access Policy query subject to obtain the configuration information about the service.

Table 42. List of query subjects in the Configuration namespace (continued)

Query subject	Description
Role Owning Credential Pool	Represents the roles that have entitlements for credential pools through a shared access policy. You must use this query subject with the Credential Pool Entitled to Shared Access Policy to obtain information about the direct and indirect roles with entitlements.
Credential Tag	Represents a credential tag corresponding to the credential pool. You must use this query subject with the query subject Credential Pool Entitled to Shared Access Policy.
Credential Pool Owner	Represents an entity that is an owner of the credential pool. The entity can be either a person owner or a role owner. You must use this query subject with the Credential Pool Entitled to Shared Access Policy.
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.

Query items for Configuration namespace

The following table lists the query items in the Configuration namespace.

Table 43. Query items in the Configuration namespace

Query subject	Query items and their description
Shared Access Policy Organization	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor The user supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit.</p>
Shared Access Policy	<p>Shared Access Policy Name The name of the shared access policy.</p> <p>Shared Access Policy Scope The scope of a shared access policy in terms of business units the policy applies. The valid values and their meanings:</p> <ul style="list-style-type: none"> • single - The policy applies to a business unit and not its subunits. • subtree - The policy applies to the subunits of a business organization. <p>Shared Access Policy Status Represents whether a policy is enabled or not. 0 represents Enabled, and 1 represents Disabled.</p> <p>Shared Access Policy Dn An LDAP distinguished name for the shared access policy.</p> <p>Shared Access Policy ID A unique numeric ID assigned to the policy by IBM Security Identity Manager system.</p> <p>Shared Access Policy Organization Dn An LDAP distinguished name for an organization to which a shared access policy applies.</p>

Table 43. Query items in the Configuration namespace (continued)

Query subject	Query items and their description
<p>Credential Entitled to Shared Access Policy</p>	<p>Credential Name The name of an account that is configured as a shared credential.</p> <p>Credential Description The description of a credential as specified in the credential configuration.</p> <p>Credential Service The name of a service to which the credential is provisioned.</p> <p>Credential Service Organization The name of an organization to which the credential service belongs.</p> <p>Credential Policy Name The name of a policy that provides the entitlements for the credential.</p> <p>Credential Shared Access Policy Membership The users or roles that have entitlement on a credential through the shared access policy. If a membership is for all the users in an organization, then All Users is displayed.</p> <p>Credential Use Global Settings A flag that indicates whether a credential uses the shared access global settings. 0 represents Uses global settings, and 1 represents Does not use global settings.</p> <p>Credential IS Searchable Indicates whether a credential is searchable or not. 0 represents Can be searched, and 1 represents cannot be searched.</p> <p>Credential IS Exclusive Indicates whether the credential is exclusive or not. You must check out an exclusive credential to view its password or other details.</p> <p>Credential IS Password Viewable Specifies whether a user can view the password on a credential. 0 represents Password is viewable, and 1 represents Password is not viewable.</p>

Table 43. Query items in the Configuration namespace (continued)

Query subject	Query items and their description
Credential Entitled to Shared Access Policy	<p>Credential Account Status The status of an account corresponding to a credential whether it is active or inactive. 0 represents Active, and 1 represents Inactive.</p> <p>Credential Reset password Indicates whether the password of a credential is regenerated with every check-in action. 0 represents Yes, and 1 represents No.</p> <p>Credential MAX Checkout Time The maximum check-out duration that is allowed for the credential in hours.</p> <p>Credential Account Dn An LDAP distinguished name for an account that is associated with a credential.</p> <p>Credential Service Organization Dn An LDAP distinguished name for an organization of a credential service.</p> <p>Credential Service Dn An LDAP distinguished name for the service on which a credential is provisioned.</p> <p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p> <p>Credential Dn An LDAP distinguished name for a credential.</p>
Credential Service	<p>Service Name The name of the service on which the credentials are provisioned.</p> <p>Service Type The profile type of the service.</p> <p>Service DN An LDAP distinguished name for the service.</p> <p>Service Business Unit Dn An LDAP distinguished name for a business unit of the service.</p>
Credential Service Organization	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor The user supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit.</p>

Table 43. Query items in the Configuration namespace (continued)

Query subject	Query items and their description
Role Owning Credentials	<p>Role Name The name of a role that is entitled to the credential.</p> <p>Role Organization Name The name of an organization to which the role belongs.</p> <p>Role Member The user members of the role.</p> <p>Role DN An LDAP distinguished name for the role.</p> <p>Role Container Dn An LDAP distinguished name for an organization to which the role belongs.</p>
Credential Pool Membership	<p>Credential Name The name of an account that is configured as a shared credential.</p> <p>Credential Dn An LDAP distinguished name for a credential.</p> <p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p> <p>Credential Pool Name The name of the credential pool.</p> <p>Credential Pool Business Unit Dn An LDAP distinguished name for a business unit of the credential pool.</p> <p>Service Name The name of the service on which the credentials are provisioned.</p>
Account	<p>Account Name The name of an account.</p> <p>Account Service Dn An LDAP distinguished name for a service that provisions an account.</p> <p>Account Status The status of an account. The valid values are Active or Inactive.</p> <p>Account Compliance The details about an account compliance. The valid values are Unknown, Compliant, Non-compliant, and Disallowed.</p> <p>Account Ownership Type The ownership type of the account. The valid values are Individual, System, Device, and Vendor.</p> <p>Account Last Access Date The last date when an account was accessed.</p> <p>Account Container Dn An LDAP distinguished name for a business unit of an account.</p>

Table 43. Query items in the Configuration namespace (continued)

Query subject	Query items and their description
Account Owner	<p>Full Name The full name of a user who owns an account.</p> <p>Last Name The surname of a user who owns an account.</p> <p>Type The profile type of the user, which is either person or business partner person.</p> <p>Status The status of a user who owns an account. Status is either Active or Inactive.</p> <p>Supervisor The supervisor of an owner, if applicable.</p> <p>Business Unit Name The name of a business unit.</p> <p>Dn An LDAP distinguished name for an owner.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit of an owner.</p>
Credential Pool Entitled to Shared Access Policy	<p>Credential Pool Name The name of the credential pool.</p> <p>Credential Pool Service The name of the service on which the groups corresponding to the credential pool are provisioned.</p> <p>Credential Pool Service Organization The name of an organization to which the credential pool service belongs.</p> <p>Credential Pool Policy Name The name of a policy that provides an entitlement for the credential pool.</p> <p>Credential Pool Shared Access Policy Membership The users or roles that have entitlement on a credential through the shared access policy. If a membership is for all the users in an organization, then All Users is displayed.</p> <p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p> <p>Credential Pool Service Dn An LDAP distinguished name for the credential pool service.</p> <p>Credential Pool Service Organization Dn An LDAP distinguished name for the organization of the credential pool service.</p>

Table 43. Query items in the Configuration namespace (continued)

Query subject	Query items and their description
<p>Credential Pool Members</p>	<p>Credential Name The name of an account that is configured as a shared credential.</p> <p>Credential Service Name The name of the service on which the credentials are provisioned.</p> <p>Credential Description The description of a credential as specified in the credential configuration.</p> <p>Credential IS Exclusive Indicates whether the credential is exclusive or not. You must check out an exclusive credential to view its password or other details.</p> <p>Credential USE Global Settings A flag that indicates whether a credential uses the shared access global settings. 0 represents Uses global settings, and 1 represents Does not use global settings.</p> <p>Credential IS Searchable Indicates whether a credential is searchable or not. 0 represents Can be searched, and 1 represents cannot be searched.</p> <p>Credential IS Password Viewable Specifies whether a user can view the password on a credential. 0 represents Password is viewable, and 1 represents Password is not viewable.</p> <p>Credential IS Checkedout Provides the status of the credentials. Yes represents that the credential is checked out, and No represents that the credential is available in the credentials vault and not yet checked out.</p> <p>Credential Account Status The status of an account corresponding to a credential whether it is active or inactive. 0 represents Active, and 1 represents Inactive.</p> <p>Credential Reset password Indicates whether the password of a credential is regenerated with every check-in action. 0 represents Yes, and 1 represents No.</p> <p>Credential MAX Checkout Time The maximum check-out duration that is allowed for the credential in hours.</p> <p>Credential Dn An LDAP distinguished name for a credential.</p> <p>Credential Account Dn An LDAP distinguished name for an account that is associated with a credential.</p> <p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p> <p>Credential Service Dn An LDAP distinguished name for the service on which a credential is provisioned.</p>

Table 43. Query items in the Configuration namespace (continued)

Query subject	Query items and their description
Credential Pool Service Organization	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor The user supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit.</p>
Credential Pool Service	<p>Service Name The name of a service on which the groups corresponding to the credential pool are provisioned.</p> <p>Service Type The profile type of the service.</p> <p>Service DN An LDAP distinguished name for the service.</p> <p>Service Business Unit Dn An LDAP distinguished name for a business unit of the service.</p>
Role Owning Credential Pool	<p>Role Name The name of a role that is entitled to the credential pool.</p> <p>Role Organization Name The name of an organization to which the role belongs.</p> <p>Role Member The user members of the role.</p> <p>Role Dn An LDAP distinguished name for the role.</p> <p>Role Container Dn An LDAP distinguished name for an organization to which the role belongs.</p>
Credential Tag	<p>Credential Dn An LDAP distinguished name for the credential.</p> <p>Credential Tag The credential tag that is associated with the credential pool.</p>
Credential Pool Owner	<p>Credential Pool Dn An LDAP distinguished name for the pool.</p> <p>Credential Pool Owner Dn An LDAP distinguished name for an owner of the credential pool.</p> <p>Credential Pool Owner Name The name of an owner of the credential pool.</p> <p>Credential Pool Owner Business Unit The name of a business unit to which the credential pool owner belongs.</p> <p>Credential Pool Owner Type Desc The type of an owner. Possible values are User and Role.</p>

Table 43. Query items in the Configuration namespace (continued)

Query subject	Query items and their description
Role Members	<p>Full Name The full name of a user who is assigned to the role.</p> <p>Last Name The surname of a user who is assigned to the role</p> <p>Type The profile type of the user, which is either person or business partner person.</p> <p>Status The status of a user who is assigned to the role. Status is either Active or Inactive.</p> <p>Supervisor The supervisor of a role member, if applicable.</p> <p>Business Unit Name The name of a business unit.</p> <p>Dn An LDAP distinguished name for a role member.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit of a role member.</p>

Application ID Configuration namespace for Application ID Module

The Configuration namespace provides the configuration level information about application, its instances and its supporting data.

Query subjects for Application ID Configuration namespace

The following table lists the query subjects in the Application ID Configuration namespace.

Table 44. List of query subjects in the Application ID Configuration namespace.

Query subject	Descriptions
Application	Represents the applications available in the system. You can use this query subject with the application instance query subject. By doing so, you can obtain configuration information about the registered instances of an application.
Application Organization	Represents the business unit to which an application belongs to. you must use this query subject with the application query subject. By doing so, you can obtain configuration information about the business unit to which an application belongs.
Application Instance	Represents the application instances available in the system. You can use this query subject with the application query subject to know the application for which the instance belongs to.
Registered Application Instance	Represents the registered applications and its instances in the system by the application ID tool. You must use this query subject with the application and application instance query subject. By doing so, you can obtain the configuration information about the registered application and instances.

Query items for Application ID Configuration namespace

The following table lists the query items in the Configuration namespace.

Table 45. Query items in the Application ID Configuration namespace.

Query subject	Query items and their description
Application	<p>Application Dn An LDAP distinguished name for the application.</p> <p>Application Name The name of the application.</p> <p>Application Business Unit Dn An LDAP distinguished name for the business unit of the selected application.</p>
Application Organization	<p>Business Unit Name The name of the business unit.</p> <p>Business Unit Supervisor The user supervisor of the business unit.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit.</p>
Application Instance	<p>Application Dn An LDAP distinguished name for the application.</p> <p>Application Instance Dn An LDAP distinguished name for the application instance.</p> <p>Application Instance Name The name of the application instance.</p>
Registered Application Instance	<p>Application Instance Name The name of the application instance.</p> <p>Application Instance Dn An LDAP distinguished name for the application instance.</p> <p>Application Instance Registrant Name The name of the user who registers the application instance.</p> <p>Application Instance Registrant Dn An LDAP distinguished name for the user who registers the application instance.</p> <p>Application Instance Description The description of the application instance.</p> <p>Application Instance Type The type of application instance. It can be a Java application, script, or a J2EE data source.</p> <p>Application Instance System Host The host name of the system where the application instance is located.</p> <p>Application Instance Fingerprint The environment and binary properties for the application instance.</p> <p>Application Instance Business Unit Dn An LDAP distinguished name for the application instance business unit.</p>

Application Instance Activity Audit namespace for Application ID Module

The Application Instance Activity Audit namespace provides the records of the credentials that are used by an application instance.

Query subjects for Application Instance Activity Audit namespace

The following table lists the query subjects in the Application Instance Activity Audit namespace.

Table 46. List of query subjects in the Application Instance Activity Audit namespace

Query subject	Descriptions
Application Instance Activity Audit	Represents the application instance activity audit records in the system. You can use this query subject to generate an audit report for credentials that are used by an application instance.
Application Instance	Represents the application instances available in the system. You can use this query subject with the Application Instance Activity Audit query subject to obtain the application instance activity audit records.
Application Instance Business Unit	Represents the application instance business units available in the system. You can use this query subject with the Application Instance Activity Audit query subject to know the application instance for which the business unit belongs to.
Credential	Represents a credential on which the audit action is performed. You must use this query subject with the Application Instance Activity Audit to obtain information about the audited credential and application instance information.
Credential Resource Business Unit	Represents a business unit that is associated to the credential resource. You must use this query subject with the credential query subject to know the credential resource for which the business unit belongs to.

Query Items for Application Instance Activity Audit namespace

The following table lists the query items in the Application Instance Activity Audit namespace.

Table 47. List of query items in the Application Instance Activity Audit namespace

Query subject	Query items and their description
Application Instance Activity Audit	<p>Audit Action The action that is performed by an application instance on the credential. The only supported action is Get Credential.</p> <p>Audit Date The date and time of the audit action</p> <p>Audit Initiator Name The name of an application instance who initiated the audit action on a credential.</p> <p>Audit Initiator Dn An LDAP distinguished name for the application instance that initiated the audit.</p> <p>Audit Credential Name The name of a credential that is used by the application instance.</p> <p>Audit Credential Dn An LDAP distinguished name for the credential.</p> <p>Audit Credential Business Unit The name of a business unit to which the credential belongs.</p> <p>Audit Result Summary The result of the audit action. The valid values are Success and Failure.</p> <p>Audit Comments The comments that are specified by a user during audit action.</p>
Application Instance	<p>Application Instance Name The name of the application instance.</p> <p>Application Instance Dn An LDAP distinguished name for the application instance.</p> <p>Application Instance Description The description of the application instance.</p> <p>Application Instance Registrant The name of the user who registers the application instance</p> <p>Application Instance Registrant Dn An LDAP distinguished name for the user who registers the application instance.</p> <p>Application Instance Type The type of application instance. It can be a Java application, script, or a J2EE data source.</p>

Table 47. List of query items in the Application Instance Activity Audit namespace (continued)

Query subject	Query items and their description
Application Instance Business Unit	<p>Business Unit Name The name of the business unit that the application instance belongs to.</p> <p>Business Unit Supervisor The user supervisor of the business unit.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit.</p>
Credential	<p>Credential Name The name of a credential on which the audit action is performed.</p> <p>Credential Dn An LDAP distinguished name for a credential.</p> <p>Credential Description The detailed description of a credential.</p> <p>Credential Resource Name The name of the credential resource.</p> <p>Credential Resource URI The identifier of the credential resource used for getting the credential.</p> <p>Credential Resource ID A unique ID that is associated with the credential resource.</p>
Credential Resource Business Unit	<p>Business Unit Name The name of a business unit to which the credential resource belongs to.</p> <p>Business Unit Supervisor The supervisor of a user who owns the business unit.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit to which the credential resource belongs to.</p> <p>Business Unit Container Dn An LDAP distinguished name for a business unit.</p>

Generating the report through IBM Cognos Business Intelligence

Each report type has its own set of search parameters to filter the report data. Use these search parameters to generate the content that meets your requirements for a selected report.

About this task

You can choose the output format of the reports. For more information about the supported report format, search **Report Formats** from the IBM Cognos Business Intelligence product documentation at <http://www.ibm.com/support/knowledgecenter/SSEP7J/welcome>.

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.
- Any time stamp in the following reports uses 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.

Procedure

1. Open IBM Cognos Connection.
2. Select the report model **ISPIMReportingModel_2.0.1**.
3. Select the specific report.
4. Specify the parameters for the report.
 - a. Enter a keyword or % in the filter field and click **Search**.
 - b. Select the values from the **Results** list and click **Insert** to add the selected parameter values to the **Choice** list.
5. Click **Finish**. The Prompt Page Summary is displayed, which provides an overview of the specified report parameters.
6. Click **Page Down** to view the details of the report.

Chapter 16. Security administration

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

View management

IBM Security Privileged 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 Privileged Identity Manager provides. For example, you might restrict the set of tasks that group members have.

Before you begin

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.

Procedure

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

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 Privileged Identity Manager provides. For example, you might restrict or expand the set of tasks that group members have.

Before you begin

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.

Procedure

1. From the navigation tree, select **Set System Security > Manage Views**.
2. On the Define Views page, in the **Name** field, type information about the view and click **Search**.
3. In the **Manage Views Results** 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

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 Privileged 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

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.

Procedure

1. From the navigation tree, select **Set System Security > Manage Views**.
2. On the Define Views page, in the **Name** field, type information about the view and click **Search**.
3. In the **Manage Views Results** 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 Privileged Identity Manager. It is defined by a unique identifier, a URL, and optional parameters. The task can be associated with IBM Security Privileged 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 Privileged Identity Manager 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 Privileged Identity Manager Service Center, it is started in the inline frame, or *iframe*, of the browser window that contains the Privileged Identity Manager 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 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 Privileged Identity Manager Service Center for the Self-service console. To turn off headers so that it integrates better with the Privileged Identity Manager Service Center, see "Customizing website layout" in the IBM Security Identity Manager product documentation

Procedure

1. From the navigation tree, select **Set System Security > Manage Views**.
2. On the Define Views page, click **Manage Custom Tasks** in the **Manage Views Results** 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, hashtags, 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 `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 Privileged Identity Manager Service Center. For example, if the identifier suffix is consoleui, then the property to add to CustomLabels.properties can be CUSTOM_CONSOLEUI = Privileged 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 CustomLabels.properties.

If you want to display Custom task as the description of the task in the Privileged Identity Manager 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 = T che Personnalis e.

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 Privileged Identity Manager Service Center, it is started in the inline frame, or *iframe*, of the browser window that contains the Privileged Identity Manager 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 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 **Manage Views Results** 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. You can define a label for the custom task by editing the `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 Privileged Identity Manager Service Center. For example, if the identifier suffix is `consoleui`, then the property to add to `CustomLabels.properties` can be `CUSTOM_CONSOLEUI = Privileged Identity Manager Console UI`.
6. 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 `CustomLabels.properties`.

If you want to display Custom task as the description of the task in the Privileged Identity Manager 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 = T che Personnalis e`.

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 Privileged Identity Manager Service Center and verify that your changes are applied.

Deleting a custom task

As an administrator, you can delete from IBM Security Privileged 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 **Manage Views Results** 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.

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 Privileged Identity Manager.
- 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 Privileged 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

Use the default access control items for shared access to manage access security.

Table 48. Default access control items for Shared Access Module

Protection category	Name	Type	Principal
Credential	Default ACI for Credential: Grant All to Account Owner	erCredential	Account Owner
Credential	Default ACI for Credential: Grant All to Domain Admin	erCredential	Domain Admin
Credential	Default ACI for Credential: Grant Search to Domain Admin/Service Owner/Supervisor/Auditor Group	erCredential	Domain Admin Service Owner Supervisor Auditor Group
Credential	Default ACI for Credential: Grant Search for Everyone	erCredential	Everyone
Credential Lease	Default ACI for Credential Lease: Grant All to Domain Admin	erCredentialLease	Domain Admin
Credential Lease	Default ACI for Credential Lease: Grant Search and CheckinForOthers to Account Owner/Supervisor/Lessee Supervisor	erCredentialLease	Account Owner Supervisor Lessee Supervisor
Credential Lease	Default ACI for Credential Lease: Grant Search to Domain Admin/Service Owner/Auditor Group	erCredentialLease	Domain Admin Service Owner Auditor Group
Credential Lease	Default ACI for Credential Lease: Grant Attribute Read/Write for Everyone	erCredentialLease	Everyone

Table 48. Default access control items for Shared Access Module (continued)

Protection category	Name	Type	Principal
Credential Pool	Default ACI for Credential Pool: Grant All to Domain Admin/Service Owner	erCredentialPool	Domain Admin Service Owner
Credential Pool	Default ACI for Credential Pool: Grant Search to Auditor Group	erCredentialPool	Auditor Group
Credential Pool	Default ACI for Credential Pool: Grant Search for Everyone	erCredentialPool	Everyone
ITIM Group	Default ACI for ITIM Group: Grant AssignGroupToPool to Domain Admin	erSystemRole	Domain Admin
Service Group	Default ACI for Service Group: Grant AssignGroupToPool to Domain Admin/Service Owner	erGroupItem	Domain Admin Service Owner
Credential Service	Default ACI for Credential Service: Grant All to Domain Admin	erCVService	Domain Admin
Shared Access Policy	Default ACI for Shared Access Policy: Grant All to Domain Admin	erSharedAccessPolicy	Domain Admin
Shared Access Policy	Default ACI for Shared Access Policy: Grant Search to Auditor Group	erSharedAccessPolicy	Auditor Group
Shared Access Policy	Default ACI for Shared Access Policy: Grant attribute to Everyone	erSharedAccessPolicy	Everyone

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

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.

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 IBM Security Privileged 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

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.

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 IBM Security Privileged 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

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.

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 Privileged 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 17. Deprecated tasks

Shared access policy and role management tasks are deprecated.

Access in IBM Security Privileged Identity Manager 2.0.1 subsumes static role, dynamic role, role access, and shared access policy in earlier versions. Shared access entitlements defined in earlier versions of IBM Security Privileged Identity Manager will continue to work.

See Table 4 on page 65.

The following topics are provided as a reference.

Role administration

Organizational roles are a method of providing users with access to managed credentials and credential pools. Organizational roles determine which credentials and pools are granted 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 a user is assigned to an organizational role, the credentials and credential pools granted to the role through shared access policy become available for the user to access.

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.

Role overview

IBM Security Privileged Identity Manager 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.

A static role can be defined as an access. If a role is defined as an access, the role membership can be requested through access request. Furthermore, the access can be optionally associated with an access request workflow with an approval or mail activity.

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

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

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 as 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**.

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

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.

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 49. 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 Privileged 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 Privileged Identity Manager administration console contains these columns with sample values and supported formats:

Table 50. 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 51. 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=5628670506891199803,ou=roles,erglobalid=000000
AIX Role	Employee;Role;Role access	Used by the customer to deploy server.	Role-grey	erglobalid=5628669752130902869,ou=roles,erglobalid=000000
Default Role	Mail;Unique ID	BVT server that is used to run BVT from developer and tester.	\$mailrisk-red	erglobalid=5628670337030215245,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 Privileged Identity Manager administrative console.

Before you begin

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 Privileged Identity Manager administrative console to import the role access data from a comma-separated value (CSV) file.

Before you begin

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.

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.

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.

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 Service Center user interface.

About this task

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

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 Privileged Identity Manager Reference Guide*.

Role assignment attributes and the Self Service or the Identity Service CenterIdentity 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 CenterIdentity 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

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

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

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

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.

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 **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

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 IBM Security Privileged 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.

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.

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.

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. Assign users to a role so that the users have access to the credentials.

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.

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.

About this task

When you add child roles to a parent role, ensure that there is not a separation of duty policy violation.

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.

About this task

When you add child roles to a parent role, ensure that there is not a separation of duty policy violation.

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

Determine how removing the role affects the role hierarchy.

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.

About this task

You can use the Manage Access Types page to create an access type.

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 Identity Service Center user interface. To do so, associate the role with the newly created access type.

Shared access policy management

Shared access policies authorize role members to share credentials or credential pools.

You can define a policy for:

- A set of specific credential pools
- A set of specific credentials
- All pools or credentials with the same organization container context
- A filter for a set of credentials or credential pools
- A combination of one or more of the items in this list

Before you work with shared access policies, create an access control item (ACI) for the protection category of Shared Access Policy. For more information about ACIs, see “Access control item management” on page 232.

Creating shared access policies

As an administrator, you can create a policy to enable credentials to be checked out so that users can check out credentials by using the self-service interface.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of Shared Access Policy. For more information about ACIs, see “Access control item management” on page 232.

Organizational roles and services that the shared access policy uses must be in place before you create the shared access policy.

If a role is a member of another organizational role in a shared access policy, then that role member also inherits the permissions of the shared access policy.

Procedure

To create a shared access policy, complete these steps:

1. From the navigation tree, select **Manage Shared Access > Manage Shared Access Policies**.
2. In the **Shared Access Policies** table, click **Create**.
3. On the General page, complete these steps:
 - a. Type the name of the policy.
 - b. Optional: Type information about the policy in the **Description** field.
 - c. Set the policy status. The status is set to **Enable** by default.
 - d. Click **Search** to specify a business unit other than the default Organizational business unit.
 - e. Select the scope that the policy uses for the business unit. The scope is set to **This business unit and its subunits** by default.
4. Click the Members page and select the member type that you want to associate with the shared access 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. Click the Entitlements page and add one or more entitlements to the shared access policy:
 - a. Click **Add**.
 - b. On the Entitlements page, select the Entitlement Target Type.
 - c. Depending on your selection, do the following.

Credential

Specify the information to limit the credential search. Leaving a field blank is the same as selecting all credentials.

- 1) Type a login ID.
- 2) Type the resource name.
- 3) Click **Search**.
- 4) Select the credentials that you want to add to the entitlement.

Credential pool

Specify the information to limit the credential pool search. Leaving a field blank is the same as selecting all credential pools.

- 1) Type the pool name or a description of the pool.
- 2) Type the resource name.
- 3) Click **Search**.
- 4) Select the credential pools that you want to add to the entitlement.

Filtered

Under **Filter Creation**:

- 1) Select the type of filter that you want to create from the list.

Credentials

- a) Use the **Select all** check box to entitle all credentials under the policy business unit. No additional information is needed. The information fields are deactivated.
- b) Type the name of the entitlement. If enabled, this field is a required field.
- c) Supply the filter information.
 - i. Type the login ID.
 - ii. Type the resource name.
 - iii. Type the resource tag.

Note: If you do not specify any filter information, the entitlement defaults to the all credentials entitlement. If you specified an entitlement name, it is overridden by the default **All credentials** name.

Credential Pools

- a) Use the **Select all** check box to entitle all credential pools under the policy business unit. No additional information is needed. The information fields are deactivated.
- b) Type the name of the entitlement. If enabled, this field is a required field.
- c) Supply the filter information:
 - i. Type the pool name.
 - ii. Type the resource name.
 - iii. Type the resource tag.

Note: If you do not specify any filter information, the entitlement defaults to the all credential pools entitlement. If you specified an entitlement name, it is overridden by the default **All credential pools** name.

- d. Click **OK**. The credentials or credential pools are displayed in the **Entitlements** table.
 - e. Click **Cancel** to return to the Entitlements page.
 - f. Click **Preview** to see the list of credentials or credential pools that are returned by the filter criteria that you specified.
6. Click **Submit** to save the policy.
 7. On the Success page, click **Close**.

Modifying shared access policies

As an administrator, you can modify a shared access policy so that you can change its definition, membership, or entitlement to meet the needs of your organization.

About this task

Ensure that you created an access control item (ACI) for the protection category of Shared Access Policy. For more information about ACIs, see “Access control item management” on page 232.

If a role is a member of another organizational role in a shared access policy, then that role member also inherits the permissions of the shared access policy.

Procedure

To modify a shared access policy, complete these steps:

1. From the navigation tree, select **Manage Shared Access > Manage Shared Access Policies**.
2. On the Manage Shared Access Policies page, type information about the shared access policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Shared Access Policies** table, select a shared access policy and click **Change**.
4. On the Manage Shared Access Policies page, modify the fields on the General, Members, and Entitlements pages.

Note: You can modify only those entitlements that have a target type of filtered credential or filtered credential pool. If you want to change other target type entitlements, you must remove and re-create the entitlements.

5. Click **Submit** to save the changes.

Note: Credentials that are currently checked out are not affected by the policy change.

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

Deleting shared access policies

As an administrator, you can delete shared access policies. Deleting a shared access policy deletes all the entitlements that are associated with the policy.

Before you begin

Ensure that you created an access control item (ACI) for the protection category of Shared Access Policy. For more information about ACIs, see “Access control item management” on page 232.

Before you delete a shared access policy, confirm that you want to delete all the memberships and entitlements in that policy.

A role might be a child role of another organizational role in a shared access policy. That child role also inherits the permissions of the shared access policy. Therefore, when you delete a shared access policy, the permissions of the child roles might be deleted or suspended.

Procedure

1. From the navigation tree, select **Manage Shared Access > Manage Shared Access Policies**.
2. On the Manage Shared Access Policies page, type information about the shared access policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Shared Access Policies** table, select a shared access policy and click **Delete**.
4. On the Confirm page, review the shared access policy to be deleted and click **Delete**.
5. On the Success page, click **Close**.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings

can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details/us/en> sections entitled "Cookies, Web Beacons and Other Technologies" and "Software Products and Software-as-a Service".



Printed in USA