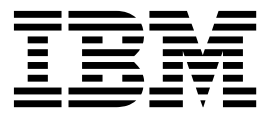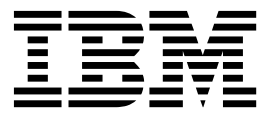IBM Security Privileged Identity Manager
Version 2.1.1

Administrator Guide

IBM

IBM Security Privileged Identity Manager
Version 2.1.1

Administrator Guide

IBM

Contents

Notices **281**

Figures

Tables

Chapter 1. Appliance Administration

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

To manage the virtual appliance, the virtual appliance administrator logs on to the **Appliance Dashboard** at `https://<ispimva_hostname>:9443`.

For more information on virtual appliance administrator tasks, see "Virtual appliance dashboard" in the *IBM Security Privileged Identity Manager Planning and Deployment Guide*.

Viewing notifications

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

Procedure

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

   ```
   Restart the Identity service
   Restart the SingleSignOn service
   Restart the SessionRecorder service
   Restart the appliance
   Middleware components not configured
   The disk space utilization has exceeded the warning threshold
   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 in the **Server Control** widget.

   ```
   Restart the Identity service
   Restart the SingleSignOn service
   Restart the SessionRecorder service
   ```

   If a message for restarting the appliance is displayed, restart the virtual machine from the menu or from the command line interface (CLI). This condition occurs if you did not restart the appliance after your first configuration or if you enable App ID after 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.

    Not applicable
        It indicates that the node is a primary node.

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.

Table 1. Synchronization states table. (continued)

State	Description	Action
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.
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.

2. 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

1. From the **Appliance Dashboard**, locate the **Server Control** widget.
2. 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.
3. Optional: Click **Refresh** to display the data again.

Viewing deployment statistics

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

Procedure

1. 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.
2. Optional: Click **Refresh** to display the data again.

Viewing server health status

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

Procedure

1. From the **Appliance Dashboard**, locate the **Status Monitor** widget.
2. Optional: Click **Refresh** to display the data again.

A service can display the following status:

- **Started** or **Stopped**

- **Available** or **Unavailable**

The **Status** for the Privileged Session Gateway might display the following status indicators:

Available
The service is fully operational.

Degraded
The service is partially operational. Some of the nodes in the cluster might not be available.

Severe
The services are in a bad state. All the nodes in the cluster are not available, or the health status cannot be determined.

Not Available
The service is not operational or the host cannot be reached.

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 the 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
   - Service Center
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. 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, `2.1.1`.

   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 event logs

System events are logged when the system settings are changed and when problems occur with the system. Use the Event Log management page to view and to export system events on your network.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor > Logs > Event Log**. The Event Log page displays system events in the **System Events** tab.

2. From the **System Events** tab, do one of the following actions.

   - Click **Pause Live Streaming** to stop the live updating of the event log.
   - Click **Start Live Streaming** to resume live updating of the event log.
   - Filter the system events with the following steps:

     a. Click **Filter** to display the Filter window.

     b. From the **Column** list, select a column name to filter on it. The column names are as follows:

        – **Any Column**
        – **Priority**
        – **Event ID**
        – **Event Description**
        – **Time Occurred**

        Note: The virtual appliance does not return results for the **Time Occurred** column when you select **Any Column**. Select the **Time Occurred** column to filter values in that column.

     c. From the **Condition** list, select a filter condition. Available filter conditions vary depending on the tab that you selected in the event log. The possible filtering conditions include these options:

        – **contains**
        – **is**
        – **starts with**
        – **ends with**
        – **before**
        – **after**
        – **range**

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

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

     e. Click **Filter**.

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

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

     Note: The default file name is export.csv.

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

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

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 **Monitor** > **Monitoring** > **Memory**. The System Memory Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 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 **Monitor** > **Monitoring** > **CPU**. The System CPU Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 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 **Monitor** > **Monitoring** > **Storage**. The Storage Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 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 which partitions that you want to review.

Boot Indicates the boot partition.

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

Managing the SNMP monitoring

You can monitor the system events of the IBM Security Privileged Identity Manager virtual appliance with SNMP.

About this task

When configured, the SNMP agent listens on the management interface.

The SNMP Monitoring function can monitor the virtual appliance in an IBM Tivoli® Monitoring environment. Use the Agentless Monitoring for Linux OS agent.

For more information about configuring the IBM Tivoli Monitoring environment and the Agentless Monitoring for Linux OS agent, see the IBM Knowledge Center.

The following management information bases, or MIBs, are used by the SNMP agent:

SNMPv2-MIB	TCP-MIB
SNMPv2-SMI	UDP-MIB
SNMP-FRAMEWORK-MIB	HOST-RESOURCES-MIB
SNMP-MPD-MIB	MTA-MIB
SNMP-TARGET-MIB	DISMAN-EVENT-MIB
SNMP-USER-BASED-SM-MIB	NOTIFICATION-LOG-MIB
SNMP-VIEW-BASED-ACM-MIB	UCD-SNMP-MIB
IF-MIB	UCD-DLMOD-MIB
IP-MIB	UCD-DISKIO-MIB
IPV6-MIB	UCD-SNMP-MIB
IP-FORWARD-MIB	NET-SNMP-AGENT-MIB
NET-SNMP-VACM-MIB	

Procedure

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

   Note: The default port number is 161.
5. Select one of these SNMP protocols.

   SNMPv1/SNMPv2c
   In the **Community** field, type the name of the community that the SNMP manager uses to authenticate with the SNMP agent.

   SNMPv3
   Configure the following options to describe the user that accesses the SNMP agent.

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

Option	Description
Privacy Protocol	From the **Privacy Protocol** list, select the privacy protocol to use.
Privacy Password	Type the password to be used as a privacy passphrase. The password must be a minimum of 8 characters in length.
Privacy Password (Confirm)	Retype the privacy password to confirm.

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

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 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 **View 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 virtual appliance. After the initial configuration, partition 1 is active and contains the firmware version of the currently 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 virtual appliance restarts the system by using partition 2, which is now the active partition.

Note: The 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 virtual machine 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**.
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 from 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 to active when you want to use the firmware that is installed on that partition. For example, you might want to set a partition to 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 virtual appliance restarts the system from 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.

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 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**.
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 the 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 virtual appliance.

Results

The following information is displayed in the About page:

```
Product Name: IBM Security Privileged Identity Manager
Product Version:      2.1.1
Server Name:          ispimva.example.com
Installed Fix Packs:  None
Build number:         20141205-1328
Build Date and Time:  Dec 5, 2015 1:32:57 AM
```

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.

Managing application interfaces

To manage application interfaces with the management interface, use the Application Interfaces page.

Before you begin

Ensure that your virtual machine has 3 network interfaces. After adding a network interface, you must reboot the virtual appliance.

About this task

An IP address and its corresponding fully qualified domain name for any application interface must have a static IP address, which must be different from the local management interface address.

Procedure

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

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

   Address
   > Indicates the address of the application interface. For example, `192.0.2.22`.

   Interface FQDN
   > Indicates the fully qualified domain name of the application interface. For example, `ispim.example.com`.

   Interface Gateway
   > Indicates the address of the network gateway to be used by the application interface. For example, `192.0.2.1`.

   Netmask/Prefix
   > Indicates the netmask or prefix of the application interface. For example, `255.255.255.0`.

   > A netmask is used for **IPv4**, and a prefix is used for **IPv6**.

2. Do one of these actions.

Table 2. Application Interfaces action items

Action	Button	Description
Add an address	New	**Note:** Ensure the IP address that you assign is not used by any other system.
		1. Click **New** to display the Add Address window.
		2. Select one of the following options to indicate the type of address to add.
		IPv4
		IPv4 defines each interface on a network uniquely. It is a 32-bit numeric address, which is written in decimal as four sets of digits that are separated by periods with no spaces or consecutive periods. Each number can be 0 - 255. For example: 192.0.2.2.
		IPv6
		IPv6 improves the efficiency of routing and provides greater security. It is a 128-bit IP address, which is written in hexadecimal and separated by colons. For example:
		2001:db8:8484:3:220:f9ff:fe25:70cf
		3. Specify the fully qualified domain name of the application interface in the **Interface FQDN** field.
		4. Specify the Interface Gateway.
		5. Do one of these actions.
		• For **IPv4 Settings**, do these steps.
		a. Type an address value in the **Address** field.
		b. Type a net mask value in the **NetMask** field.
		• For the **IPv6 settings**, do these steps.
		a. Type an address value in the **Address** field.
		b. From a range of 0-64, specify a prefix value in the **Prefix** field.
		6. Click **Save**.
		7. If any notifications are displayed in the **Notifications** widget, take appropriate actions as necessary.
		A message indicates that the application address is added successfully, and the record is listed in the **Interface 1** table.

Table 2. Application Interfaces action items (continued)

Action	Button	Description
Edit an address	**Edit**	1. Select the address. 2. Click **Edit** to display the Edit Address window. 3. Specify the fully qualified domain name of the application interface in the **Interface FQDN** field. 4. Specify the Interface Gateway. 5. Do one of these actions. • For **IPv4 Settings**, do these steps. a. Edit address value in the **Address** field. b. Edit net mask value in the **NetMask** field. • For **IPv6 Settings**, do these steps. a. Edit address value in the **Address** field. b. Edit prefix value in the **Prefix** field. 6. Click **Save**. A message indicates that the address is updated successfully.
Delete an address	**Delete**	1. Select an application interface. 2. Select the address. 3. Click **Delete** to display the Confirm Action window. 4. Click **Yes**. A message indicates that the address is deleted successfully.
Test a connection	**Test**	1. Click **Test** to display the Ping Server window. 2. In **Server**, enter the IP address or name of the server to test the connection. 3. Click **Test**. A message indicates whether the test connection was successful or not.
Refresh the application interface data	**Refresh**	Click **Refresh** to display the most recent version of the data, including changes that were made to the data since it was last refreshed.

3. Click **Save Configuration**.

Managing the hosts file

To manage hosts file with the IBM Security Privileged Identity Manager virtual appliance, use the Manage Hosts File page.

Procedure

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

> **Address**
>> Specify the IP address of the host record.
>
> **Host Name**
>> Specify the host name of the host record.
>
>> d. Click **Save**.
>
> • Add a host name to a host record
>> a. Select a host record entry to add the host name to.
>>
>> b. Click **New**.
>>
>> c. On the Add Hostname to Host Record page, enter the host name.
>>
>> d. Click **Save**.
>
> • Remove a host record
>> a. Select a host record entry to delete.
>>
>> b. Click **Delete**.
>>
>> c. On the confirmation page, click **Yes** to confirm the deletion.
>
> • Remove a host name from a host record
>> a. Select host name entry to delete.
>>
>> b. Click **Delete**.
>>
>> c. On the confirmation page, click **Yes** to confirm the deletion.
>
>> **Note:** If the removed host name is the only associated host name for the IP address, then the entire host record (the IP address and host name) is removed.
>
> • Refresh the data
>
>> Click **Refresh** to display the most recent version of the data since it was last refreshed.

Managing IBM Security Directory Integrator instances

IBM Security Privileged Identity Manager uses IBM Security Identity Adapters to communicate with various managed resources. These adapters are deployed and run on instances of the Security Directory Integrator.

About this task

The appliance has two pre-configured Security Directory Integrator instances. You can install new adapters only on the "SDIServer2" instance.

Important:

Configuration of a new adapter **must** be on service port 2099.

Before you install or upgrade to a new adapter, ensure that the adapter supports backward compatibility.

Changes that you make to the Directory Integrator instance are propagated to the nodes in a cluster by the node synchronization process.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**. The Security Directory Integrator Management page displays a table with these column names.

Instance ID
> Specifies the ID that was assigned to the instance when it was created. For example, the initial instance is SDI1.

Instance Name
> Specifies the name of Security Directory Integrator instance. For example, SDIServer1.

State Indicates whether the instance is started or stopped.

Changes are Active
> Indicates whether the adapters in the Security Directory Integrator instance are functioning.

Port Indicates the port that the instance listens on. For example, 1099.

2. On the Security Directory Integrator Management page, do one of these actions.

Table 3. Security Directory Integrator action items

Action	Button	Description
Edit an instance	**Edit**	1. Select the instance. 2. Click **Edit** to display the Edit Security Directory Integrator Server window. 3. Use the up and down arrows to change the minimum amount of memory that you want to assign to the instance in the **Minimum Heapsize(MB)** field. The minimum `heapsize` is, 256. 4. Use the up and down arrows to change the maximum amount of memory that you want to assign to the instance in the **Maximum Heapsize(MB)** field. The maximum `heapsize` is, 4,096. 5. Click **Save Configuration**. A message indicates that the Security Directory Integrator server is being edited. After the server instance changes are complete, a system notification message is displayed that the instance update is successful.
Start an instance	**Start**	1. Select the instance. 2. Click **Start**. A message indicates that the Security Directory Integrator server is starting. After the server instance is started, a system notification message is displayed that the instance started successfully.
Stop an instance	**Stop**	1. Select the instance. 2. Click **Stop**. A message indicates that the Security Directory Integrator server is stopping. After the server instance is stopped, a system notification message is displayed that the instance stopped successfully. **Note:** You can only stop the "SDIServer2" instance.

Table 3. Security Directory Integrator action items (continued)

Action	Button	Description
Restart an instance	**Restart**	1. Select the instance. 2. Click **Restart**. A message indicates that the Security Directory Integrator server is restarting. After the server instance is restarted, a system notification message is displayed that the instance was restarted successfully.
Refresh the instance data	**Refresh**	Click **Refresh** to display the most recent version of the data, including changes that were made to the data since it was last refreshed.
Troubleshoot instance problems, configure instance properties files, install adapters, and manage the instance certificates	Manage	1. Select the instance. 2. Click **Manage**. • Click **Troubleshooting** > **Log tracing** to access and retrieve system logs. See "Managing log configuration" in the *IBM Security Identity Manager Installation and Configuration Guide*. • Click **Troubleshooting** > **View log** to see the Security Directory Integrator server log. • Click **Configuration** > **solution.properties** to manage the Dispatcher `solution.properties` file. See "Configuring the Dispatcher properties for the Directory Integrator instance." • Click **Configuration** > **itim_listener.properties** to manage the Dispatcher `itim_listener.properties` file. See "Configuring the Dispatcher properties for the Directory Integrator instance." • Click **Certificates** to manage the server certificate. See "Managing Certificates" in the *IBM Security Identity Manager Installation and Configuration Guide*. • Click **SDI Adapters** to install, uninstall, or export adapters. See "Managing IBM Security Directory Integrator adapters" on page 19

Configuring the Dispatcher properties for the Directory Integrator instance

The Dispatcher is a Security Directory Integrator component. It enables the IBM Security Privileged Identity Manager Server to communicate with IBM Tivoli Directory Integrator-based adapters. You can modify the `solution.properties` and `itim_listener. properties` files that configure the Dispatcher.

About this task

The `solution.properties` and `itim_listener. properties` files can be modified on the primary or a stand-alone node only. In cluster environments, the nodes must be synchronized for the Directory Integrator instance configuration changes to propagate to the secondary and member nodes.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**.

2. Select the instance for the Dispatcher that you want to manage and click **Manage** > **Configure**.
3. Select the Dispatcher property file that you want to manage.
   - **solution.properties**
   - **itim_listener.properties**

   The SDI Advanced Configuration window is displayed with these tabs.

   ALL   Displays the properties that are contained in the file and their assigned values.

   Modified
   Displays the properties that were changed with their new values, their default value, and indicates whether they are new properties.
4. Perform any of the following actions.

Table 4. Security Directory Integrator property actions

Action	Button	Description
Add a property	**New**	1. On the All tab, click **New** to display the Update property window. 2. Specify the name of the property that you want to create. 3. Specify the value for the property. 4. Click **Save Configuration**. A message indicates that a new SDI property is being created. After the property is created, a system notification message is displayed and the property is added to the All and Modified table.
Change a property value	**Edit**	1. From either tab, select the property. 2. Click **Edit** to display the Update property window. 3. Specify the new value for the property. 4. Click **Save Configuration**. A message indicates that the SDI property is being updated. After the property is updated, a system notification message is displayed and the property value is updated on the All table and the property is added to the Modified table.
Delete a property	**Delete**	**Note:** You can delete customer-added properties. Installed properties cannot be deleted. If you try to delete a required property, the operation fails. 1. From the Modified tab, select the property. 2. Click **Delete** to display the Remove SDI Property window. 3. A confirmation message is displayed. Click **Yes** to delete the property. A message indicates that the property server is being removed. After the property is deleted, a system notification message is displayed that the instance is deleted.

5. When you are finished, click **Close**.

Managing IBM Security Directory Integrator adapters

You can install and uninstall Security Directory Integrator adapters through the virtual appliance. The adapters enable IBM Security Privileged Identity Manager to communicate with various resources.

Before you begin

You must download the adapter package from the IBM Passport Advantage website. Go to http://www.ibm.com/software/how-to-buy/passportadvantage/pao_customers.htm.

About this task

If you have a cluster environment, adapter management tasks must be performed on the primary node. The adapter management tasks that are performed on a directory integrator instance propagate to the same instance on each node in the cluster during node synchronization.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**.
2. Select the **SDI Server 2 instance** and click **Manage** > **SDI Adapters** The SDI Adapters window is displayed with a table that list the name, version, and any comments about the installed adapters.
3. Perform any of the following actions.

Table 5. Security Directory Integrator adapter actions

Action	Button	Description
Add an adapter	**Install**	1. Click **Install**. 2. Click **Browse** and navigate to the adapter package that you want to install. 3. Click **OK**. A message indicates that a new SDI adapter is being installed. After the adapter is installed, a system notification message is displayed and the adapter is added to the SDI Adapters table. **Note:** Ensure that you restart the SDI instance after installing the adapter. See "Restart the instance" in "Managing IBM Security Directory Integrator instances" on page 16.
Uninstall an adapter.	**Uninstall**	1. Select the adapter. 2. Click **Uninstall** to display the Remove SDI Adapter window. 3. A confirmation message is displayed. Click **Yes** to delete the adapter. A message indicates that the adapter is being removed. After the adapter is deleted, a system notification message is displayed and the adapter is removed from the table.
Download an `adapter.zip` bundle	**Export**	1. Select the adapter. 2. Click **Download**. 3. Select to save the file. 4. Click **OK**. The file is saved to your download directory.

4. When you are finished, click **Close**.

Configuring static routes

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

About this task

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

Procedure

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

Table 6. Static route actions

Field	Action
IPv4 Default Gateway	1. Specify an address value. For example: `192.0.2.0`. 2. Click **Save**. **Note:** Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.
IPv6 Default Gateway	1. Specify an address value. For example: `2001:DB8:0000:0000:02AB:00FF:FE29:9C6A`. 2. Click **Save**. **Note:** Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.
New	1. Click **New** to create a route. 2. In the Add Route window, define values in these fields. • **Destination** • **Gateway** • **Metric** • **Interface or Segment** 3. Click **Save Configuration**.
Edit	1. Select an existing route. 2. Click **Edit** to change the settings. 3. In the Edit Route window, edit values in these fields. • **Destination** • **Gateway** • **Metric** • **Interface or Segment** 4. Click **Save Configuration**.
Delete	1. Select an existing route. 2. Click **Delete**. 3. Click **Yes** to confirm your action.

Results

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

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

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

Option	Description
Date	Specifies the day, month, and year for the IBM Security 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 (Network Time Protocol) servers that the IBM Security Privileged Identity Manager virtual appliance uses. You can enter multiple NTP servers, which are separated by commas.

3. Click **Save Configuration**.
4. 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.

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. 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 information that might compromise the security of your virtual appliance, 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.

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

As a System Administrator, 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 Privileged Access 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.

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.

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, the Privileged Administrator group and the Privileged Session Recorder Auditor group.

Creating user profiles

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

Before you begin

If you need to place a new user on a business unit, create the business unit first.

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. 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.

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. 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 temporarily has no need to access IBM Security Privileged Identity Manager, you can suspend the 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 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, the user cannot log in to all IBM Security Privileged Identity Manager consoles or applications. Restoring a suspended 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**.
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.

User Password management

There are two ways to manage user 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

Important: If the IBM Security Privileged Identity Manager virtual appliance is configured to authenticate users against an external user registry, do not use the following password management feature. This password management feature does not apply when an external user registry is configured.

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.

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. 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**.

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

Important: If the IBM Security Privileged Identity Manager virtual appliance is configured to authenticate users against an external user registry, do not use the following password management feature. This password management feature does not apply when an external user registry is configured.

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.

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. 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.

b. Click **Submit**.

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

Delegate activities

You can delegate activities to another user during a time when a user is 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. The logged-in user must have the access control item permission to write the delegate attribute of the user who is delegated.

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

You can create a delegation schedule to delegate the activities of a 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.

About this task

This task is available only for administrators and cannot be customized. This task does not apply if an external user registry is configured. If another user registry is specified, the number of login attempts is managed by the external user registry.

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

As a System Administrator, you can control how user passwords can be changed,and reset.

Note: User password administration is not applicable if the virtual appliance is configured to use an external user registry.

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
- 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 recovery
- Disallowing specific passwords

Password expiry can be set on the user settings.

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 resets

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.

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.

About this task

This option is intended to enable prompting for a password when creating users through the user interface. 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.

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 a custom validation rule

Create a custom validation rule to evaluate a password after the other rules are defined in the **Rules** tab.

About this task

To define a custom password validation rule, type a Javascript function `validate(password)`. The function shall return an error message if the password is not acceptable. If the password is valid, the function shall return a `null` or `undefined` message.

Note: This task is optional. You only need to create a custom validation rule if the built in password rules in "Password strength rules" on page 39 cannot satisfy your requirements.

Procedure

1. Log in to the Administrative console.
2. From the navigation tree, select **Manage Password Policies**.
3. Click **Create**.
4. In the **Custom Rule** tab, type a Javascript function `validate(password)`. For example, the following function checks if a password contains 3 uppercase characters or 3 lowercase characters:

```
    function validate(pwd) {
      var lc = 3, uc = 3;

      for (var c in pwd.split('')) {
        if (c >= 'a' && c <= 'z') {
          lc++;
        }
        if (c >= 'A' && c <= 'Z') {
          uc++;
        }
      }

      if (uc < 3 && lc < 3) {
        return 'Password must contain at least' +
          '3 uppercase or 3 lowercase characters';
      }
    }
```
5. Click **OK**.

Enabling forgotten password recovery

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.

To recover a forgotten password, a user must respond to a set of forgotten password questions with answers that the user previously specified. Responses are not case-sensitive by default. This is controlled by *enrole.challengeresponse.responseConvertCase* property from the `enRole.properties` file. If you want answers to be case-sensitive, change the value for *enrole.challengeresponse.responseConvertCase* 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 user-defined questions to predefined questions, users 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 password recovery challenges.

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 password recovery challenges.

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**.

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. Password policies can be applied to user passwords and to generated passwords of shared credentials.

Before you begin

Besides the system administrator, Service owner group members can view this task and create password policies for the identity providers. 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.
   - To set password policy for users, select the **Default password policy for ISPIM Service**.
   - To set password policy for identity providers, create or change a password policy and 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.

Password strength rules

Password strength rules a password policy uses to determine whether a password is valid.

The following table describes each password strength rule:

Table 7. Password Strength Rules

Attribute	Description
Maximum length	Enter the maximum number of characters for a password. For example: If the value of this rule set to 6, the password length must not exceed 6 characters.
Minimum length	Enter the minimum number of characters for a password. For example: If the value of this rule set to 12, the password must have at least 12 characters.

Table 7. Password Strength Rules (continued)

Attribute	Description
Maximum repeated characters	Enter the maximum number of times that a character can repeat consecutively in the password. For example: If the value of this rule is 2, the user can add `PPaPP` as part of the password.
Minimum unique characters	Enter the minimum number of unique characters for a password. For example: If the value of this rule is 3, the password must have at least 3 unique characters, such as `abcdcba`.
Minimum alphabetic characters	Enter the minimum number of alphabetic characters for a password. For example: If the value of this rule is 3, the password must have at least 3 alphabets, such as `a1b2c3d`.
Minimum numeric characters	Enter the minimum number of numeric characters for a password. For example: If the value of this rule is 3, the password must have at least 3 numbers, such as `a1b2c3d`.
Minimum lowercase characters	Enter the minimum number of lowercase characters for a password. If you require the password to be in all lowercase, use the "Restricted to characters" rule instead. For example: If the value of this rule is 3, the password must have at least 3 lowercase characters, such as `a1b2c3D`.
Minimum uppercase characters	Enter the minimum number of uppercase characters for a password. If you require the password to be in all uppercase, use the "Restricted to characters" rule instead. For example: If the value of this rule is 3, the password must have at least 3 uppercase characters, such as `A1B2c3D`.

Characters not allowed	Enter characters that are not allowed in the password. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a disallowed character.
	
	For example: If you want to specify _-|{}& and * as disallowed characters, a correct value for this field is:
	`_- |{}&*`
	
	An incorrect value for this field is:
	`_ - | { } & *`
	
	or:
	`_,-,|,{,},&,*`

Table 7. Password Strength Rules (continued)

Attribute	Description

Required characters	Enter a set of characters from which at least one of the characters must be in the password.
	Note: Do **not** separate any characters with a space or another delimiter, unless a space or the delimiter is a character that must be specified.
	
	For example, when this rule is used for generating passwords, the generated password can be one of the following:
	1. Contains 'a' only
	`llalll`
	2. Contains 'a' and 'b'
	`alabll`
	3. Contains 'a', 'b', and 'c'
	`acabcc`

Restricted to characters	Enter the set of characters to which the password is restricted. The password must contain only these characters. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a character that must be specified.
	
	For example, if you want to specify all lowercase letters, a correct value for this field is:
	`abcdefghijklmnopqrstuvwxyz`
	
	An incorrect value for this field is:
	`a b c d e f g h i j k l m n o p r s t u v  w x y z`
	
	or
	`a,b,c,d,e,f,g,h,i,j,k,,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z`

Starts with characters	Enter the sequence of characters, one of which must be the first character of the password.
	Note: Do **not** separate any characters with a space or another delimiter, unless a space or the delimiter is a character that must be specified.
	
	For example, if you want to specify that a password should start with 1 or 2 or 3 or 4, the generated password can be:
	`1abcde`
	`1234de`
	
	or
	`432c23`

Repeated history length	Enter the number of passwords that are retained. This value specifies how many unique passwords must be used before a previous password can be re-used. Passwords that match any password in the history list cannot be reused. The history is updated every time the password is changed. For example, specify a value of 7 so that the password must be changed 7 times to a different password before the old password can be reused.

Table 7. Password Strength Rules (continued)

Attribute	Description
Reversed history length	Enter the numeric value that specifies how many passwords, spelled backwards are kept in history. Passwords that match any password in the history list cannot be re-used. The history is updated every time the password is changed. For example, specify a value of 7 so that the password must be changed 7 times to a different password before the old password (spelled backwards) can be re-used.
Disallow user name	Select the check box to prevent the user name to have the same value as the password. The comparison is case sensitive. For example, if the user name is John, then the user is not allowed to set a password containing the word John.
Disallow user name (case-insensitive)	Select the check box to prevent the user name to have the same value as the password. The comparison is not case sensitive. For example, if the user name is John, then the user is not allowed to set a password containing the word John, john, johN, or any variation of John as part of the password.
Disallow user ID	Select the check box to prevent the user ID to have the same value as a password. The comparison is case sensitive. For example, if the user ID is JSmith, then the user is not allowed to set a password containing word JSmith. Since the comparison is case-sensitive, the user can have Jsmith, jsmith, or other variations as part of the password.
Disallow user ID (case-insensitive)	Select the check box to prevent the user ID to have the same value as a password. The comparison is not case sensitive. For example, if the user ID is JSmith, then the user is not allowed to set a password containing the word JSmith, Jsmith, jsmith, or other variations as part of the password.
Passwords must contain characters from three of the following four categories: • Uppercase letter A through Z • Lowercase letter a through z • Number 0 through 9 • Nonalphanumeric characters: ~!@#$%^&*_-+=`|\ (){}[]:;"'<>,.?/	Select the check box to enable the use of three of the mentioned four categories.

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.

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. You must create an admin domain to manage shared credentials.

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.

Administrative domains

An *administrative domain* (admin domain) identifies a subsidiary part of an organization as a separate entity.

Credentials, resources, identity providers, access, and applications are managed under administrative domains.

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, in the administrator console, in the organization tree, for an Admin Domain node. Then, the IBM Security Privileged

Identity Manager user is granted the appropriate rights based on access control items (ACI) 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 administrator is usually a system administrator. Other users can be given 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 of an Admin 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 rights to do administration tasks in that domain.

Procedure

1. In the administrative console, from the navigation tree, select **Manage Organization Structure**.
2. If an Admin Domain does not exist, create it.
   a. Click the icon next to the **Organization** node, and then click **Create Admin Domain**. The Admin Domain Details page is displayed.
   b. Type the Admin Domain name. For example: JKE Datacenter A
3. Click **Search** to locate a user.
4. On the Select People page, select the check box for the user or users that you want to make domain administrators for the Admin Domain, and click **OK**.
5. Click **OK** on the Admin Domain Details page.

Creating a node in an organization tree

As a system 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 shared access management or user management.

Changing a node in an organization tree

As a system 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

Shared access administration provides centralized management of shared privileged credentials. It enables sharing of credentials among multiple users.

This section only applies to the Privileged Administrator for on-boarding and managing shared credentials, managing resources, managing identity providers, managing access, and managing application identities.

You can store credentials (user ID and password or SSH Keys) in a credential vault. Grant users access to these credentials by specifying the access entitlement. See "Access management" on page 70 to learn more about the types of access entitlements.

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. You can define a credential tag or a set of credential tags in a credential pool. Credentials that share the same set of credential tags 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.

You can also grant users access to credential pools by specifying access entitlement. See "Access management" on page 70 to learn more about the types of access entitlements.

Table 8 describes data references that you can use during administration tasks.

Table 8. Data reference for shared access

Data Reference	Description
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, `audit_event`, which contains fields common to all audit events.

Credential management

From the Privileged Identity Manager Service Center, a privileged administrator can create, modify, and delete credentials, specify the credential type, and connect it to an identity provider so that you can rotate passwords or SSH Keys automatically on the resource.

A privileged administrator can specify one of the following credential type when creating a credential:

Password-authenticated credential
Credentials that require passwords to authenticate into privileged accounts.

SSH Key-authenticated credential
Credentials that require SSH keys to authenticate into privileged accounts.

Note: A credential with the same name can be assigned to both types of credential. For example, cred1 can be a password-authenticated credential and an SSH key-authenticated credential. See "Adding credentials in the Privileged Identity Manager Service Center" on page 51.

Connected and disconnected credentials

Credentials can exist in the credential vault as connected or disconnected credentials.

Connected
Connected credentials are associated with an identity provider, with an equivalent Identity adapter available for the target system. You can manage passwords or SSH Keys of these credentials, such as configure automatic password or SSH Key rotation, which is often a compliance requirement.

Disconnected
Disconnected credentials exist as standalone objects (user ID and password or SSH Key) in the credential vault. These credentials simply use the credential vault as secure, controlled storage. You cannot configure automatic password or SSH Key rotation for disconnected credentials.

You typically want to configure connected credentials. For example, in deployments where users can view passwords or download SSH Keys in the self-service console, and the password or SSH Key is known by a IBM Security Privileged Identity Manager user, you want to rotate the password or SSH Key automatically to minimize the risk exposure window. You can do this by enabling **Change password or key upon check in**.

You can on-board disconnected credentials, in cases where an Identity adapter is not available for the target system. To mitigate the lack of automatic password or SSH Key rotation, consider the following options:

* Configure the credentials for automatic logon with Privileged Access Agent or Privileged Session Gateway. Disable the **Allow view password or key download to user** option for the self-service console.

  Note: Privileged Access Agent does **not** support SSH Key credentials
* Perform periodic manual password rotation on the target systems, and manually update the passwords that are stored in IBM Security Privileged Identity Manager.

  Note: SSH Keys that are stored in IBM Security Privileged Identity Manager cannot be updated.

Table 9. Tasks for connected and disconnected credentials

Connected	Disconnected
"Adding credentials in the Privileged Identity Manager Service Center" on page 51	"Adding credentials in the Privileged Identity Manager Service Center" on page 51
"Connecting a credential to an identity provider" on page 55	
"Resetting credential passwords and SSH Keys" on page 55	

Table 9. Tasks for connected and disconnected credentials (continued)

Connected	Disconnected
"Configuring a reset interval for credentials" on page 57	
"Disconnecting a credential from an identity provider" on page 57	

Exclusive and non-exclusive credentials

Exclusive credentials are privileged credentials that require check-out and can only be used by one user at a time. Non-exclusive credentials can be used concurrently by multiple users and are configured to not require check-outs.

It is recommended to configure exclusive credentials, which are credentials that require check-out.

Benefits of exclusive credentials:
- Accountability and forensics. Only a single user can use the credential at a time.
- Auditability. Allows the user enter a justification for using the credential.
- Security. Allows passwords or SSH Keys of credentials to be rotated by enabling **Change password or key upon check in** in the Administrative console.

Benefits of non-exclusive credentials:
- Used in App ID scenarios. For the application identity management scenarios, where credentials are consumed by applications, credentials must be configured to not require checkouts.
- Only a single privileged credential available on the target system. For example, network devices only offer a single fixed `admin` privileged credential, but different users require concurrent access to this single privileged credential.

Table 10. Tasks for exclusive and non-exclusive credentials

Exclusive credentials	Non-exclusive credentials
"Configuring the credential default settings" on page 111	"Configuring the credential default settings" on page 111
	"Specifying non-exclusive shared access credentials" on page 58
"Checking in credentials in a credential pool" on page 63	Chapter 8, "Application identity management," on page 125

Adding credentials in the Privileged Identity Manager Service Center

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

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 exist on the target system and added separately.

Procedure

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

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

   Note: Credential type is shown in the **Manage Credential** page where credentials are listed.

   Password
   > Select this option to enable password input for the credential.

   Confirm Password
   > Re-enter the credential password that you provided in the previous field.

   SSH Key
   > Select this option to enable the credential to request for an SSH Key.

   > **Upload**
   >> Click this button to upload a private key file.

   > **Private key passphrase**
   >> Specify the passphrase for the private key file you uploaded in the previous field. If there is no password for the private key file, leave the field empty.

   > **Public key (optional)**
   >> Specify a public key.

   >> **Note:** A public key is not always needed. Most of the time, it can be derived from the private key.

   Resource
   > Select the resource that the credential belongs to.

   > If the resource does not exist, click **Add** to create a resource and specify the resource aliases, the specified host names, and IP addresses of the resources.

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

   Reset Interval (Days)
   > Specify a reset interval for each credential so that passwords or SSH Keys for a credential expire within a length of time and must be reset.

   > **Note:** Reset interval only takes effect after the credential is connected to an Identity Provider.

Credential Tag

Identifies any tag that references the credential. Credential tags are used when you are creating credential pools.

Sharing options

Select one of the following settings:

Use default setting

If you want to use the default settings for your system for sharing credentials, select this option.

One user at a time

If you want to share the credential exclusively, select this option. Users must check out the credential to use it. If you select this option, only one user at a time can check out the credential.

Multiple users or applications

Select this option to share the credential non-exclusively or enable the credential for use in applications.

Note: If this option is selected, users are not required to check out the credential to use it.

No sharing

The credential is stored in the credential vault but it is not shared. privileged users are not able to access the credential.

4. Click **Add** to display more rows 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 or credential type 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.

Note: If you are modifying an SSH Key credential, you cannot edit the SSH Key file.

6. Click **Save**.

Deleting credentials

As a privileged administrator, you can delete credentials in your domain.

About this task

This task deletes credentials in your domain. The credentials are also removed automatically from all access that reference them. If all credentials referenced by an access are deleted, the entire access 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 or credential type by using the **Filter By** option.
3. Select one or more credentials that you want to delete.
4. Click **Delete**.

Viewing password history for credentials

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

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 280.

   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, click 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**.

Resetting credential passwords and SSH Keys

Resetting credential passwords or SSH Keys changes the passwords or SSH Keys of a credential. As a privileged administrator, you can reset credential passwords or SSH Keys, depending on the credential type.

Before you begin

Ensure that the credential that you want to reset the password or the SSH Key for 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 or credential type by using the **Filter By** option.

3. Select one or more connected credentials that you want to reset the password or SSH Key.

4. Click **Reset Password/Key**.

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 reset the password or SSH Key of the credential.

Before you begin

Add a credential that is not connected to an identity provider. See "Adding credentials in the Privileged Identity Manager Service Center" on page 51.

There must be an existing identity provider to which you can connect the credential. See "Adding identity providers" on page 67.

There must be an account on the endpoint that is represented by an identity provider on IBM Security Privileged Identity Manager 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.

About this task

When you connect a credential to an identity provider, the password for both the credential and the account on the endpoint can be reset by the system so that they are the same.

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 or credential type 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.

   Note: You can only select Identity Providers that match the credential type.
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 Options page, complete the following steps:
   a. Select one of the following options:
      - **Password credentials:**

        Generate a new password (preferred choice)
        Select this option to have the system reset the password for the credential and the account when the system connects them. This option is preferred and provides the highest 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.

- **SSH Key credentials:**

  Generate a new SSH Key now (preferred choice)
  > Select this option if you want the system to reset the SSH Key for the credential and the account when the system connects them. This option is preferred and provides the highest security.

  Do not change the SSH Key
  > Select this option if you want the SSH Key to remain the same when the credential is connected to the account.

  b. The **Change password upon check in** or **Rotate SSH Key upon check in** check box is selected by default. When the check box is selected, the password or SSH Key is changed in the managed resource when the credential is checked in. If you do not want the password or SSH Key to be changed when the credential is checked in, clear the check box. 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 or the SSH Key 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 or credential type 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 a reset interval for credentials

Set a reset interval for each credential so that passwords or SSH Keys for a credential expire within a length of time and must be reset. You can apply password or SSH Key rotation to credentials by using the Service Center. Periodic rotation can only be performed on connected credentials.

About this task

Periodic rotation is useful for credentials that are used in application identity management scenarios. These credentials are non-exclusive and do not require check-out.

For passwords or SSH Keys to rotate automatically, you must also configure a rotation lifecycle rule. The rotation lifecycle rule specifies how often the rule should check for credentials that are due for a password or SSH Key reset.

To restrict the number of credentials that are rotated per cycle, configure the enRole.properties parameter com.ibm.ispim.passwordRotation.maxCredsRotatePerCycle. The default value is 200. If the value is set to -1, there is no limit to the number of credentials that are rotated per cycle. Resetting a large number of credentials can overload IBM Security Privileged Identity Manager. The property guards against such a scenario. For example, this scenario might occur if you have a large set of credentials, which have the same rotation interval, and the credentials are on-boarded at the same time. By limiting the number of credentials that are rotated per cycle, the rotation timing for the credentials are staggered across multiple cycles in a steady state. Tune this parameter according to your server performance. See Managing server properties.

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 **Reset Interval** column, specify the number of days.
5. Click **Save**.

Configuring a lifecycle rule

You can configure a rule to check for credentials that are due for password or SSH Key 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 or SSH Key resets daily every 12 hours.

Specifying non-exclusive shared access credentials

Take the following steps to define a non-exclusive credential for a shared access credential by using either the administrative console or Service Center.

Procedure

• Define the non-exclusive credential in Service Center.
    1. Start the Service Center.
    2. Select **Manage Credentials**.
    3. Select a credential that you want to define as a non-exclusive credential and click **Edit**.
    4. Select the **Credential Settings** row.
    5. Select **Multiple users or applications**.
    6. Click **Save**.

- Define the non-exclusive credential in the administrative console.
  1. Start the IBM Security Privileged Identity Manager administrative console.
  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 274.

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.

Creating credential pools

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

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. In the **Authenticator Type** drop-down list, specify whether the credential pool is for Password credentials or SSH Key credentials.
   d. For the **Resource** field, click **Search** to select for a resource for the credential pool.
   e. On the Select Resource page, search for and select a resource and click **OK**. The resource name is displayed in the **Resource** field.
   f. For the **Business unit** field, click **Search** to select a business unit for the credential pool.
   g. 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.
   h. 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**.

i. 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

Specify tags of credentials that you want to add into the pools.

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.

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 tag-based rule for the pool.

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. In the **Authenticator Type** list, select the credential pool type.
   d. For the **Resource** field, click **Search** to select for a resource for the credential pool.
   e. On the Select a Resource page, search for and select a resource and click **OK**. The resource name is displayed in the **Resource** field.
   f. For the **Business unit** field, click **Search** to select a business unit for the credential pool.
   g. 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.
   h. 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**.

i. 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 automated check-out or check-in with Privileged Access Agent.

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. After you check in a credential, any existing Privileged Session Gateway sessions that are associated with the credential are terminated.

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

A resource represents an endpoint, such as a network server or a network device.

An example of a resource is a Linux server. Its hostname or an IP address can be specified as resource which is used to connect to the endpoint using Privileged Access Agent or Privileged Session Gateway.

Adding resources

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

About this task

You can also add resources when you add a credential. See "Adding credentials in the Privileged Identity Manager Service Center" on page 51.

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 type
   > Choose one of the following types of resources:
   > - **Active Directory** - The credential belongs to a domain.
   > - **Windows Local** - The credential are local Windows account.
   > - **Database** - The credential belongs to a database.
   >
   >   Note: This resource can be used in integration with IBM Cognos®.
   > - **Generic** - Other credential types.
   >
   > according to the type of credentials that you plan to manage. If the credentials belong to a domain, choose **Active Directory**. If the credentials are local Windows accounts, choose **Windows Local**. For other credential types, choose **Generic**.

   Resource name
   > Type a name for the resource. This is used for searching credentials and can be used to link the credential to an access.

   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 access entitlements. If your access entitlement has a matching resource tag, the credential is available for check-out. You can specify multiple resource tags.

Results

The added resource is displayed on the Managed Resources page.

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 cannot modify the Resource UID. You can use this field for shared bulk load operations. See "Shared access bulk upload" on page 74.

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**.

   Note: You cannot delete a resource when there are existing credentials or entity associations to it. To delete a resource, you must remove the credential or entity association before proceeding with the deletion.

Identity provider management

Identity providers let you manage passwords or SSH Keys of privileged accounts that reside on managed endpoints, such as servers or network devices.

To use an identity provider, you add an identity provider entity to establish trust between the managed endpoint and IBM Security Privileged Identity Manager.

The identity provider automates the following tasks:
- Changing credential passwords and SSH Keys.
- 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 11. Identity providers for managed resources.

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

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**.

   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. Click **Test Connection** to verify that the identity provider settings are correct. Connection verification is recommended.

Modifying an 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**.

   Note: Reenter the password upon each update and test the connection before
   you submit the changes made to an identity provider.

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**.

OpenSSHKeyProviderService Identity Provider

As a Privileged Administrator, you can create an SSH Key authenticated identity
provider from the Privileged Identity Manager Service Center to manage SSH Keys
of privileged accounts.

The OpenSSHKeyProviderService Identity Provider automates the rotation of
credential keys. To automate the rotation, connect an SSH Key credential to this
identity provider. The selection of the available list of identity providers depends
on the credential type. For example, if the credential that you are connecting is an
SSH Key credential, the list only shows the OpenSSHKeyProviderService identity
provider.

Note:
- You cannot connect multiple credentials that are of both password and SSH Key
  credential type at the same time.
- Only SSH Key credentials can be connected to a OpenSSHKeyProviderService
  identity provider.
- `Admin-mode` uses the administrator credential to rotate connected credentials.
  When you test the connection of the identity provider to the host that is
  specified, the administrator credential is used.
- `Self-mode` uses the connected credential to rotate its own key. When you test the
  connection of the identity provider to the host that is specified, select one of the
  available SSH Key credentials to test the connection.

To create an OpenSSHKeyProviderService identity provider, provide the following
information:

Tab	
General Information	**Service name** Specify a name for the Identity Provider. It is used in the list of available identity providers at the **Connect Credential** page. **Host** Specify the host name or IP address of the target endpoint, that is accessed using the SSH Key. **Description** Optional: Specify a description that identifies the service for your environment. **Path to `authorized_keys` file** Optional: Specify the file path to the `authorized_keys` file. • Be default, if this field is left empty, the location of the `authorized_keys` file is the location that is configured in the host SSH Server configuration file, `sshd_config`. • If the `authorized_keys` file configuration option in the `sshd_config` is not configured, the default location, `%h/.ssh/authorized_keys`, is used to locate the `authorized_keys` file. • If the `authorized_keys` file configuration option is configured to a custom path but the `sshd_config` file has restricted read permissions, this field must be filled in with the correct custom file path to use self-mode. **Note:** The system-wide `authorized_keys` file path that does not contain `%h` or `%u` is **not** accepted. **Administrator credential** Optional: This field must be specified if you are want to run this identity provider in `admin-mode`. If the field is left empty, it is in `self-mode`. **Note:** The SSH Key credentials must be valid SSH Keys to the host. The administrator credential is used to rotate the connected credentials. Type in the field or click **Advanced Search** to search for the SSH Key credential to use. **Is sudo user?** Optional: Select this check box if the administrator credential that is specified requires sudo to execute privileged commands. **Owner** Optional: Select one of the available users from the list. If the field is left empty, by default, the owner is the Privileged Administrator that is creating the identity provider

Tab	
Forwarder	Use Forwarder if IBM Security Privileged Identity Manager is unable to reach the host machine directly. For example, when the host machine is connected to a private network. **Important:** The forwarder must have Netcat (nc) installed. If you are using Forwarder, ensure that you complete the following fields: **Host** Specify the hostname of the forwarding server. **Credential to connect** Specify the SSH Key credential for IBM Security Privileged Identity Manager to connect to the forwarder.

Status and Information	**Last connecting time**
	    Displays the time of creation of the identity provider or the last time that any SSH Key was attempted to be rotated.
	
	Last successful connecting time
	    Displays the time of creation of the identity provider or the last time SSH Key was successfully rotated.

Access management

Access is the permission for privileged users to use a set of managed credentials on resources.

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

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.

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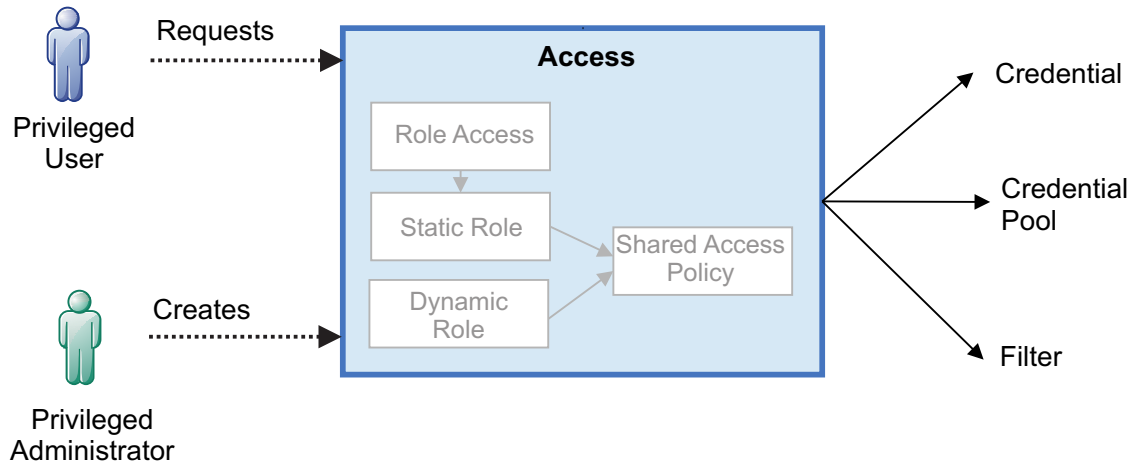
Figure 1. Privileged administrators grant users access to resources with a simplified entitlement model

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

Table 12. 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 13. 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).

Table 13. Person attributes for an LDAP filter (continued)

Attribute	Description
`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))`

4. 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 72, determines the available options on the page.

5. 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.
>
> **Note:** The **Type** column lists the type of credentials. For example, `Password` or `SSH Key`. You can add entitlements to credentials of different types in one access.

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 upload

As a privileged administrator, you can upload credentials, credential pools, identity provider and application services with a CSV file. You can also modify information for the credentials, credential pools, identity provider and application services. IBM Security Privileged Identity Manager uses the settings that are indicated in a CSV file to add or update the credentials, credential pools, identity provider and application services.

Bulk load operations

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

Note: On boarding of SSH Key credentials are **not** applicable with bulk upload.

A 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
- Adding managed application services in bulk
- Modifying managed application services in bulk
- Adding identity providers in bulk
- Modifying identity providers in bulk
- Connecting credentials to identity providers in bulk
- Disconnecting credentials from identity providers in bulk
- Adding resources in bulk
- Modifying resources in bulk
- Adding access in bulk
- Modifying access in bulk

Format of the bulk upload CSV file

A bulk upload 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
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`, `#IdentityProviders`, or `#ManagedInstances`.

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: For information about the column headers, see the following topics:
- "`#Credentials_v2` type identifier column headers" on page 99
- "#CredentialPools_v2 type identifier column headers" on page 101
- "#ManagedInstances type identifier column headers" on page 107
- "#IdentityProviders type identifier column headers" on page 81
- "`#Resources` type identifier column headers" on page 76
- "**#Access** type identifier column headers" on page 103

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

Table 14. What you can upload with the administrative console and Service Center.

If your CSV file contains	Use	See
`#Credentials_V2, #CredentialPools_V2,` `#IdentityProviders, or #Resources`	Administrative console	"Uploading a CSV file with the administrative console" on page 110
`#ManagedInstances and #Credentials_V2`	Service Center	"Uploading a CSV file for application services with Service Center" on page 146

See "Example CSV file with credentials and identity providers" on page 108 for more information on uploading a CSV file.

#Resources type identifier column headers

The `#Resources` type identifier allows you to handle bulk upload of resources.

Each type identifier line must contain a resource type identifier. It is represented in the following form:

`#Resources, <resource type>`

For example, `#Resources,winlocal`

the following resource types are available:
- `Generic` for **Generic** resource type uploads
- `WinLocal` for **WinLocal** resource type uploads
- `Database` for **Database** resource type uploads

The following generic headers apply to all identity providers: ORG_PDN, RESOURCE_UID, RESOURCE_NAME, RESOURCE_TAG, and RESOURCE_ALIAS. See the resource types for an explanation for each of these headers. In addition to the generic headers, there is a set of property headers unique to each resource type.

Generic resource type:

Learn about the resource column headers for bulk loading of **Generic** resource type uploads.

Attribute column header	Description	Required
ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)` You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input. It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location China, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required
RESOURCE_UID	Specifies the resource unique ID.	Required
RESOURCE_NAME	Specifies the resource name.	Required
RESOURCE_TAG	Specifies one or multiple resource tags, if any. For example, `tag1|tag2|tag3`.	Optional
RESOURCE_ALIAS	Specifies one or multiple resource aliases, if any. For example, `alias1|alias2|alias3`	Optional

RESOURCE_PDN	RESOURCE_PDN is a query string for the system to search for qualified resources.
	
	The following BNF notation represents the syntax for RESOURCE_PDN:
	
	`resourceRdn ::= uid '=' string (Must be a valid uid string)`
	
	You must specify a RESOURCE_PDN which can uniquely identify a resource. If the specified RESOURCE_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.
	
	For example:
	
	`uid=pim_database_79`
	
	Note: The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.
		Required, only when you are updating a resource

Example

```
#Resources
ORG_PDN,RESOURCE_UID, RESOURCE_NAME, RESOURCE_TAG, RESOURCE_ALIAS
"ou=Vic Workspace,o=PIM", "uid_build_server", "build-server", "windows",
"10.1.13.124"
```

WinLocal resource type:

Learn about the resource column headers for bulk loading of **WinLocal** resource type uploads.

Attribute column header	Description	Required
`ORG_PDN`	`ORG_PDN` is a query string for the system to search for qualified admin domains. 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.)`  You must specify an `ORG_PDN` which can uniquely identify an admin domain. If the specified `ORG_PDN` resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input.  It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location `China`, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements:  `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required
`RESOURCE_UID`	Specifies the resource unique ID.	Required
`RESOURCE_NAME`	Specifies the resource name.	Required
`RESOURCE_TAG`	Specifies one or multiple resource tags, if any. For example, `tag1|tag2|tag3`.	Optional
`RESOURCE_ALIAS`	Specifies one or multiple resource aliases, if any. For example, `alias1|alias2|alias3`.	Optional

`RESOURCE_PDN`	`RESOURCE_PDN` is a query string for the system to search for qualified resources.
	
	The following BNF notation represents the syntax for `RESOURCE_PDN`:
	
	`resourceRdn ::= uid '=' string (Must be a valid uid string)`
	
	You must specify a `RESOURCE_PDN` which can uniquely identify a resource. If the specified `RESOURCE_PDN` resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.
	
	For example:
	
	`uid=pim_database_79`
	
	Note: The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.
		Required, only when you are updating a resource

`HOST_NAME`	Specifies the database hostname.	Required for **WinLocal**

Example

```
#Resources,winlocal
ORG_PDN,RESOURCE_UID, RESOURCE_NAME, RESOURCE_TAG, RESOURCE_ALIAS, HOST_NAME
"ou=Vic Workspace,o=PIM", "uid_winlocal", "winlocal", "windows|build_machine",
"10.1.13.234", daily_build
```

`WinAD` resource type:

Learn about the resource column headers for bulk loading of **WinAD** resource type uploads.

Attribute column header	Description	Required
ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)` You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input. It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location China, for organization IBM, use "ou=Valerie Workspace, ou=HR, l=China, o=IBM". You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required
RESOURCE_UID	Specifies the resource unique ID.	Required
RESOURCE_NAME	Specifies the resource name.	Required
RESOURCE_TAG	Specifies one or multiple resource tags, if any. For example, tag1|tag2|tag3.	Optional
RESOURCE_ALIAS	Specifies one or multiple resource aliases, if any. For example, alias1|alias2|alias3.	Optional
Domain_NetBIOS_name	Specifies the name that is used by earlier versions of Windows to identify the domain.	Required for **Active Directory**
Domain_DNS_name	Specifies the full DNS name of the domain.	Required for **Active Directory**

Example

```
#Resources,winad
ORG_PDN,RESOURCE_UID,RESOURCE_NAME,RESOURCE_TAG,RESOURCE_ALIAS,DNS,NETBIOS
"ou=Vic Workspace,o=PIM" ,uid_winad,"AD controller for PIM, winad|windows-server,
10.1.13.222, pim.local, pim
```

Note: Ensure that the data line in the CSV file is in a single line.

Database resource type:

Learn about the resource column headers for bulk loading of **Database** resource type uploads.

Attribute column header	Description	Required

ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)`
	
	You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input.
	
	It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location `China`, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`.
	You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements:
	
	`o=<Organization Name>`
	`l=<Location Name>`
	`ou=<Organization Unit>`
	
	You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.
		Required

RESOURCE_UID	Specifies the resource unique ID.	Required
RESOURCE_NAME	Specifies the resource name.	Required
RESOURCE_TAG	Specifies one or multiple resource tags, if any. For example, tag1|tag2|tag3.	Optional
RESOURCE_ALIAS	Specifies one or multiple resource aliases, if any. For example, `alias1|alias2|alias3`	Optional

RESOURCE_PDN	RESOURCE_PDN is a query string for the system to search for qualified resources.
	
	The following BNF notation represents the syntax for RESOURCE_PDN:
	
	`resourceRdn ::= uid '=' string (Must be a valid uid string)`
	
	You must specify a RESOURCE_PDN which can uniquely identify a resource. If the specified RESOURCE_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.
	
	For example:
	
	`uid=pim_database_79`
	
	Note: The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.
		Required, only when you are updating a resource

HOST_NAME	Specifies the database hostname.	Optional for **Database**
DATABASE_TYPE	Specifies one of the following database types: • **db2** • **oracle** • **microsoftSqlServer** • **others**	Required for **Database**
IP	Specifies the database IP address.	Required for **Database**
PORT	Specifies the database port.	Required for **Database**

Example 1

The following sample CSV file contains information for a **Database** resource type upload:

```
#Resources,database
ORG_PDN,RESOURCE_UID, RESOURCE_NAME, RESOURCE_TAG, RESOURCE_ALIAS, DATABASE_TYPE, IP, PORT
"ou=Vic Workspace,o=PIM", "uid_database", "PIM-autobvt-db2", "autobvt|windows",
"10.127.13.21|pim-data-tier", db2, 10.127.13.21, 50050
```

Example 2

The following sample CSV file contains information to modify a **Database** resource type:

```
#Resources,database
RESOURCE_PDN, RESOURCE_NAME, RESOURCE_TAG, RESOURCE_ALIAS, IP
"uid=uid_database", "PIM-autobvt-db2-modified", "autobvt|win-server-2012", "10.1.13.13", 10.1.13.13
```

#IdentityProviders type identifier column headers

The #IdentityProviders type identifier lets you bulk load identity providers.

Each type identifier line must contain a subtype identifier, which is represented in the following form:

`#IdentityProviders,<subtype>`

For example: `#IdentityProviders,WINDOWS_LOCAL`

The following subtypes are available:
- `AD` for **ADprofile**
- `LDAP` for **LdapProfile**
- `POSIX_AIX` for **PosixAixProfile**
- `POSIX_HPUX` for **PosixHpuxProfile**
- `POSIX_LINUX` for **PosixLinuxProfile**
- `SOFTLAYER` for **SoftLayerProfile**
- `POSIX_SOLARIS` for **PosixSolarisProfile**
- `SQL2000` for **SQL2000Profile**
- `WINDOWS_LOCAL` for **WinLocalProfile**

For other adapter profiles that are not listed here, use the name of the service profile as the subtype. You can find the name of the service profile in Service Center. Click **Manage Identity Providers**, and see the list of profiles under **All Identity Providers**.

Note: Bulk upload of **OpenSSHKeyProvider** identity provider is not supported.

The following generic headers apply to all identity providers: **ORG_PDN**, **ORG_URI**, **IDENTITY_PROVIDER_PDN**, and **TEST_CONNECTION**. See the subtypes for an explanation for each of these headers. In addition to the generic headers, each identity provider will have its own set of property headers.

The headers are not case-sensitive.

AD subtype:

Know about the identity provider column headers for bulk loading of Active Directory identity providers.

Attribute column header	Description	Required
`ORG_PDN`	`ORG_PDN` is a query string for the system to search for qualified admin domains. 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.)`  You must specify an `ORG_PDN` which can uniquely identify an admin domain. If the specified `ORG_PDN` resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input.  It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location `China`, for organization `IBM`, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements:  `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required. See note. You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
`ORG_URI`	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
`IDENTITY_PROVIDER_PDN`	`IDENTITY_PROVIDER_PDN` is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for `IDENTITY_PROVIDER_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`  You must specify an `IDENTITY_PROVIDER_PDN` which can uniquely identify an identity provider. If the specified `IDENTITY_PROVIDER_PDN` resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  For example:  `erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`  where `<idp attribute>=<value>,<full path of the admin domain>` **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
`SERVICENAME`	Name to display on the user interface.	Required.
`URL`	URL of the data source. Supported protocols include: http, and https. This attribute is required.	Required.
`UID`	An identifier used to uniquely identify an identity provider.	Required.
`PASSWORD`	A password used to authenticate a user.	Required.
`TEST_CONNECTION`	Value `true` or `false`. Specify whether to test the connection before creating or updating the identity provider. If set to `true`, an identity provider is created or updated only if a connection test is successful. If `false`, the identity provider is created or updated without a connection test.	Optional. The default is set to **True**.
`DESCRIPTION`	Describe the service.	Optional.

Attribute column header	Description	Required
ADBASEPOINT	Specify the DN of the domain name, extended to allow any base point.	Optional.
ADGROUPBASEPOINT	Specify the DN of the domain name for group management.	Optional.
ADDOMAINUSER	Specify the user ID that is used when connecting to the Active Directory.	Optional.
ADDOMAINPASSWORD	Specify the password for the user ID that is used to connect to the Active Directory.	Optional.
OWNER	Specify the owner of the resource.	Optional.
URI	Identify the names of the resource.	Optional.

Example 1 - Adding an entry

```
#IdentityProviders,AD
SERVICENAME,DESCRIPTION,URL,UID,PASSWORD,ORG_PDN
"PIMQA AD Server","Domain Controller for PIMQA","http://192.0.2.24",
agent,agent,"ou=Valerie Workspace,ou=HR,l=China,o=IBM"
```

Example 2- Updating an entry

```
#IdentityProviders,AD
IDENTITY_PROVIDER_PDN,SERVICENAME,DESCRIPTION,URL,UID,PASSWORD
"erServiceName=PIMQA AD Server,ou=Valerie Workspace,ou=HR,l=China,o=IBM",
"Domain Controller for PIMQA","http://192.0.2.24",agent,new_secret
```

LDAP subtype:

Know about the identity provider column headers for bulk loading LDAP identity providers.

Attribute column headers	Description	Required
ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)` You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input. It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit `HR`, with location `China`, for organization `IBM`, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
ORG_URI	Specify the organizational container under which the identity provider 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 are 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.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

Attribute column headers	Description	Required
IDENTITY_PROVIDER_PDN	IDENTITY_PROVIDER_PDN is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for IDENTITY_PROVIDER_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`  You must specify an IDENTITY_PROVIDER_PDN which can uniquely identify an identity provider. If the specified IDENTITY_PROVIDER_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  For example:  `erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`  where `<idp attribute>=<value>,<full path of the admin domain>` **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
SERVICENAME	Name to display on the user interface.	Required.
ITDIURL	Specify the URL for the Tivoli Directory Integrator instance. Valid syntax is`rmi://ip-address:port/ITDIDispatcher`, where ip-address is the Tivoli Directory Integrator host, and port is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`.	Required.
RESOURCEURL	Specify the location and port number of the IBM Directory Server or Sun ONE Directory Server. Valid syntax is `ldap://ip-address:port`, where ip-address is the IBM Directory Server or Sun ONE Directory Server host and port is the IBM Directory Server or Sun ONE Directory Server port number. For example, you might specify the URL as `ldap://irvas02.eng.irvine.example.com:389`.	Required.
AUTHENTICATEMODE	If the authentication mode is set to **Self**, the administrator name or password is not required before you test the connection. If the authentication mode is set to **Admin**, you must specify the administrator name and password.	Required
SERVICEUID	An identifier used to uniquely identify a user of an identity provider.	Required.
PASSWORD	A password used to authenticate a user.	Required.
DSNAME	Specify the directory server type. • **OpenLDAP** - returns a null value for the venderVersion attribute. The null value causes the entire Test Connection operation to fail. • **Other** - avoids the null value error because the adapter returns a string value of `Custom code needed` for the **venderVersion** attribute. Customizing the code is a requirement only if you want to provide a valid value for the **venderVersion** attribute.	Required.
USERCONTAINERDN	Specify the full distinguished name (DN) of the container or base point where the users are stored. The adapter creates new users under this DN. Also, search operations return user account entries under this DN. For example, you might specify the DN as `ou=people,dc=com`.	Required.
LDAPUSERDN	Specify the relative distinguished name (RDN) attribute for users' LDAP entries. The RDN is a static attribute for LDAP entries and must not be modified between operation.	Required.
TEST_CONNECTION	Value `true` or `false`. Specify whether to test the connection before creating or updating the identity provider. If set to `true`, an identity provider is created or updated only if a connection test is successful. If `false`, the identity provider is created or updated without a connection test.	Optional. The default is set to **True**.
DESCRIPTION	Describe the service.	Optional.
LDAPUSESSL	Specify whether to use SSL-enabled communication between Tivoli Directory Integrator and the managed LDAP resource.	Optional.
LDAPPWDPOLENABLED	Specify whether password management policies are enabled on the directory server.	Optional.
OWNER	Specify the owner of the resource.	Optional.
LDAPALFILESYSTEMPATH	Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Privileged Identity Manager. You can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles`. Alternatively, you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating system: system: `/opt/IBM/TDI/V7.1/profiles`.	Optional.

Attribute column headers	Description	Required
LDAPMAXCONNECTIONCNT	Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter 10 if you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter 0, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.	Optional.
LDAPDISABLEALCACHE	Specify true to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.	Optional.

Example 1 - Adding an entry

```
#IdentityProviders,LDAP
ORG_PDN,TEST_CONNECTION,DSNAME,PASSWORD,SERVICENAME,SERVICEUID,URL,
DESCRIPTION
"ou=Valerie Workspace,ou=HR,l=China,o=IBM",false,no_secret,LDAP service,
admin,192.0.2.12,QA test
```

Example 2 - Updating an entry

```
#IdentityProviders,LDAP
 IDENTITY_PROVIDER_PDN,TEST_CONNECTION,Password
 "erservicename=LDAP service,ou=Valerie Workspace,ou=HR,l=China,o=IBM ",
false,new_secret
```

POSIX_AIX subtype:

Know about the identity provider column headers for bulk loading POSIX_AIX identity providers.

Attribute column header	Description	Required
ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)` You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input. It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named Valerie Workspace that belongs to the Organization Unit HR, with location China, for organization IBM, use "ou=Valerie Workspace, ou=HR, l=China, o=IBM". You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

Attribute column header	Description	Required
ORG_URI	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
IDENTITY_PROVIDER_PDN	IDENTITY_PROVIDER_PDN is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for IDENTITY_PROVIDER_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`  You must specify an IDENTITY_PROVIDER_PDN which can uniquely identify an identity provider. If the specified IDENTITY_PROVIDER_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  For example: `erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`  where `<idp attribute>=<value>,<full path of the admin domain>` **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
SERVICENAME	Name to display on the user interface.	Required.
SERVICEUID	An identifier used to uniquely identify a user of an identity provider.	Required.
AUTHENTICATEMODE	The mode of authentication with the identity provider. The valid value for **Admin** mode is "0" and "1" for **Self** mode. Regardless of **Admin** or **Self** mode, the **SERVICEUID** must be defined. For Self mode, the value of **SERVICEUID** is "Self". For Admin mode, the **SERVICEUID** is the administrator's user ID. If the authentication mode is set to **Self**, the administrator name or password is not required before you test the connection. If the authentication mode is set to **Admin**, you must specify the administrator name and password.	Required.
URL	Specify the host name or IP address for the resource. For IPv6 addresses, enter the address value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`.	Required.
TEST_CONNECTION	Value `true` or `false`. Specify whether to test the connection before creating or updating the identity provider. If set to `true`, an identity provider is created or updated only if a connection test is successful. If `false`, the identity provider is created or updated without a connection test.	Optional. The default is set to **True**.
DESCRIPTION	Describe the service.	Optional.
ITDIURL	Specify the URL for the Tivoli Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where `ip-address` is the Tivoli Directory Integrator host, and `port` is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`.	Optional.
POSIXRXATIMEOUTVALUE	Specify a value, in milliseconds, to control how long the adapter waits for a response after a remote command is issued to a managed resource. Modify this default if value operations on the managed resource timeout frequently.	Optional.
POSIXUSERREGISTRY	Specify how to manage and authenticate users. • Leave Blank if the users on the service are to be managed only through the `/etc/password` file • Type `files` if this is a mixed setup and the users are to be managed through the `/etc/password` file. • Type `LDAP` if this is a mixed setup and the users are to be managed through LDAP.	Optional.

Attribute column header	Description	Required
POSIXHOMEDIRREMOVE	Specify where to delete the home directory of the user on the AIX server when the account is deleted. Values: `true` or `false`.	Required.
POSIXRETURNSUDOPRIVILEGES	Specify whether the adapter returns the sudo privileges granted to users and groups during reconciliation. Values: `true` or `false`.	Optional.
POSIXSUDOERSPATH	If it is not the default location `/etc/sudoers` on the resource, enter the directory path to the `sudoers` file.	Optional.
OWNER	Specify the owner of the resource.	Optional.
POSIXUSESUDO	Specify whether the administrator has sudo capability on the AIX server. Values: `true` or `false`.	Optional.
POSIXAUTHMETHOD	Select the authentication method. **Password Based Authentication** uses a password to authenticate users. **Key Based Authentication** requires the use of a passphrase and private key file to authenticate users.	Optional.
PASSWORD	A password used to authenticate a user.	Optional.
POSIXPASSPHRASE	Enter the passphrase to use for key based authentication. Required for key based authentication.	Optional.
POSIXPKFILE	Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.	Optional.
POSIXALFILESYSTEMPATH	Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Privileged Identity Manager. You can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles`. Alternatively, you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux operating system: system: `/opt/IBM/TDI/V7.1/profiles`.	Optional.
POSIXMAXCONNECTIONCNT	Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter `10` if you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter `0`, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.	Optional.
POSIXDISABLEALCACHE	Specify `true` to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.	Optional.

`POSIX_HPUX` subtype:

Know about the identity provider column headers for bulk loading `POSIX_HPUX` identity providers.

Attribute column header	Description	Required
ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)` You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input. It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location China, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

Attribute column header	Description	Required
ORG_URI	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
IDENTITY_PROVIDER_PDN	IDENTITY_PROVIDER_PDN is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for IDENTITY_PROVIDER_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`  You must specify an IDENTITY_PROVIDER_PDN which can uniquely identify an identity provider. If the specified IDENTITY_PROVIDER_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  For example:  `erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`  `where <idp attribute>=<value>,<full path of the admin domain>` **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
SERVICENAME	Name to display on the user interface.	Required.
DESCRIPTION	Describe the service.	Required.
SERVICEUID	An identifier used to uniquely identify a user of an identity provider.	Required
URL	Specify the host name or IP address for the resource. For IPv6 addresses, enter the address value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`.	Required.
TEST_CONNECTION	Value `true` or `false`. Specify whether to test the connection before creating or updating the identity provider. If set to `true`, an identity provider is created or updated only if a connection test is successful. If `false`, the identity provider is created or updated without a connection test.	Optional. The default is set to **True**.
ITDIURL	Specify the URL for the Tivoli Directory Integrator instance. Valid syntax `isrmi://ip-address:port/ITDIDispatcher`, where ip-address is the Tivoli Directory Integrator host, and `port` is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`.	Optional.
POSIXUSESUDO	Specify whether the administrator has sudo capability on the HP-UX server. Values : `true` or `false`.	Optional.
POSIXEXECUTEUSERPROFILE	Specify the administrative user ID, such as root, for the HP-UX server.	Optional.
POSIXAUTHMETHOD	Select the authentication method. **Password Based Authentication** uses a password to authenticate users. **Key Based Authentication** requires the use of a passphrase and private key file to authenticate users.	Optional.
POSIXHOMEDIRREMOVE	Specify whether to delete the home directory of the user on the Linux server when the account is deleted. Values: `true` or `false`	Required.
POSIXUSESHADOW	Specify whether shadow passwords are enabled on the managed resource. This field applies to service forms only when you use the Linux or HP-UX identity providers. Values: `true` or `false`. For Linux operating systems, shadow passwords are enabled by default. When you create a service for HP-UX, by default the field is enabled. If the HP-UX system you are connecting to is an HP-UX trusted system, then the field is irrelevant and the adapter ignores the field.	Required.
PASSWORD	Specify the password for the account.	Optional.
POSIXPASSPHRASE	Enter the passphrase to use for key based authentication. Required for key based authentication.	Optional.

Attribute column header	Description	Required
`POSIXPKFILE`	Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.	Optional.
`POSIXFILESYSTEMPATH`	Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Privileged Identity Manager. You can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles`. Alternatively, you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux operating system: system: `/opt/IBM/TDI/V7.1/profiles`.	Optional.
`POSIXMAXCONNECTIONCNT`	Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter 10 if you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter 0, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.	Optional.
`POSIXDISABLEALCACHE`	Specify `true` to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.	Optional.

POSIX_LINUX subtype:

Know about the identity provider column headers for bulk loading `POSIX_LINUX` identity providers.

Attribute column header	Description	Required

`ORG_PDN`	`ORG_PDN` is a query string for the system to search for qualified admin domains. 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.)`
	
	You must specify an `ORG_PDN` which can uniquely identify an admin domain. If the specified `ORG_PDN` resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input.
	
	It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit `HR`, with location `China`, for organization `IBM`, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements:
	
	`o=<Organization Name>`
	`l=<Location Name>`
	`ou=<Organization Unit>`
	
	You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.
		Required. See note.
		
		You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

`ORG_URI`	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

Attribute column header	Description	Required
IDENTITY_PROVIDER_PDN	IDENTITY_PROVIDER_PDN is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for IDENTITY_PROVIDER_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 You must specify an IDENTITY_PROVIDER_PDN which can uniquely identify an identity provider. If the specified IDENTITY_PROVIDER_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input. For example: erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM where <idp attribute>=<value>,<full path of the admin domain> **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
SERVICEUID	An identifier used to uniquely identify a user of an identity provider.	Required.
SERVICENAME	Name to display on the user interface.	Required.
DESCRIPTION	Describe the service.	Required.
ITDIURL	Specify the URL for the Tivoli Directory Integrator instance. Valid syntax isrmi://ip-address:port/ITDIDispatcher, where ip-address is the Tivoli Directory Integrator host, and port is the port number for the RMI Dispatcher. For example, you might specify the URL as rmi://localhost:16231/ITDIDispatcher.	Required.
TEST_CONNECTION	Value true or false. Specify whether to test the connection before creating or updating the identity provider. If set to true, an identity provider is created or updated only if a connection test is successful. If false, the identity provider is created or updated without a connection test.	Optional. The default is set to **True**.
AUTHENTICATEMODE	The mode of authentication with the identity provider. The valid value for **Admin** mode is "0" and "1" for **Self** mode. Regardless of **Admin** or **Self** mode, the **SERVICEUID** must be defined. For Self mode, the value of **SERVICEUID** is "Self". For Admin mode, the **SERVICEUID** is the administrator's user ID. If the authentication mode is set to **Self**, the administrator name or password is not required before you test the connection. If the authentication mode is set to **Admin**, you must specify the administrator name and password.	Required.
URL	Specify the host name or IP address for the resource. For IPv6 addresses, enter the address value in brackets. An example of a URL using IPv6 would be http://[address]:port number.	Optional.
OWNER	Specify the owner of the resource.	Optional.
URL	URL of the data source. Supported protocols include: http, and https. This attribute is required.	Optional.
POSIXUSESUDO	Specify if the administrator has sudo capability on the Linux server. Values: true or false.	Optional.
POSIXEXECUTEUSRPROFILE	Specify the existing user ID of the service owner that administers the Linux service instance.	Optional.
POSIXAUTHMETHOD	Select the authentication method. **Password Based Authentication** uses a password to authenticate users. **Key Based Authentication** requires the use of a passphrase and private key file to authenticate users.	Optional.
PASSWORD	A password used to authenticate a user.	Optional.
POSIXPASSPHRASE	Enter the passphrase to use for key based authentication. Required for key based authentication.	Optional.
POSIXPKFILE	Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.	Optional.
POSIXALFILESYSTEMPATH	Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Privileged Identity Manager. You can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: c:\Files\IBM\TDI\V7.1\profiles. Alternatively, you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating system: system: /opt/IBM/TDI/V7.1/profiles.	Optional.

Attribute column header	Description	Required
POSIXMAXCONNECTIONCNT	Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter 10 if you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter 0, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.	Optional.
POSIXDISABLEALCACHE	Specify true to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.	Optional.
POSIXHOMEDIRREMOVE	Specify whether to delete the home directory of the user on the Linux server when the account is deleted. Values: true or false	Required.
POSIXUSESHADOW	Specify whether shadow passwords are enabled on the managed resource. This field applies to service forms only when you use the Linux or HP-UX identity providers. Values: true or false. For Linux operating systems, shadow passwords are enabled by default. When you create a service for HP-UX, by default the field is enabled. If the HP-UX system you are connecting to is an HP-UX trusted system, then the field is irrelevant and the adapter ignores the field.	Required.
POSIXRETURNSUDOPRIVILEGES	If enabled, the adapter returns the sudo privileges granted to users and groups during reconciliation. Values: true or false.	Optional.
POSIXSUDOERSPATH	If it is not the default location /etc/sudoers on the resource, enter the directory path to the sudoers file.	Optional.
POSIXFAILEDLOGINCMD	Specify the system command that is used to detect and tally failed login attempts and enforce account lockout. This command must be configured through the PAM mechanism. If no value is specified, the default **faillog** command is used. **Note:** This command is not available on some operating systems, such as RHEL 6.1 and later versions, and might cause connection attempts to fail. Therefore, specify a proper failed login command that exists on the strain of Linux installed at the target system.	Optional.
POSIXFAILEDLOGINTALLYLOC	Specify the absolute path to the location of the failed login attempt datastore, if it is not the default datastore. This field applies to **faillock** and **pam_tally2** only. The field is ignored when **faillog** is used. If you use **faillock**, specify the directory that contains the login record files for individual users. If you use **pam_tally2**, specify the full path of the file that contains the login record data for all users.	Optional.
POSIXMAXFAILEDLOGINS	Specify the maximum number of failed logins that can occur before an account is locked. This field applies to **faillock** and **pam_tally2** only. The field is ignored when **faillog** is used.	Optional.

Example 1 - adding an entry

```
#IdentityProviders,POSIX_LINUX
SERVICENAME, DESCRIPTION, URL, SERVICEUID, PASSWORD,POSIXUSESHADOW,AUTHENTICATEMODE,
POSIXHOMEDIRREMOVE,ORG_PDN
DB2Linux,"DB2 server on Linux", 192.0.0.4, root, no_secret,false,0,false,
"ou=Valerie Workspace, ou=HR, l=China, o=IBM"
```

Example 2- updating an entry

```
#IdentityProviders, POSIX_LINUX
IDENTITY_PROVIDER_PDN, SERVICENAME, DESCRIPTION
"erservicename= DB2Linux, ou=Valerie Workspace, ou=HR, l=China, o=IBM" ,
" DB2Linux ", "This is an update."
```

POSIX_SOLARIS subtype:

Know about the identity provider column headers for bulk loading POSIX_SOLARIS identity providers.

Attribute column header	Description	Required

`ORG_PDN`	`ORG_PDN` is a query string for the system to search for qualified admin domains. 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.)`
	
	You must specify an `ORG_PDN` which can uniquely identify an admin domain. If the specified `ORG_PDN` resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input.
	
	It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location `China`, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements:
	
	`o=<Organization Name>`
	`l=<Location Name>`
	`ou=<Organization Unit>`
	
	You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.
		Required. See note.
		
		You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

`ORG_URI`	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

`IDENTITY_PROVIDER_PDN`	`IDENTITY_PROVIDER_PDN` is a query string for the system to search for qualified identity providers.
	
	The following pseudo Backus-Naur Form (BNF) notation represents the syntax for `IDENTITY_PROVIDER_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`
	
	You must specify an `IDENTITY_PROVIDER_PDN` which can uniquely identify an identity provider. If the specified `IDENTITY_PROVIDER_PDN` resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.
	
	For example:
	
	`erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`
	
	where `<idp attribute>=<value>,<full path of the admin domain>`
	Note: The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.
		Required only when you are updating an identity provider.

`SERVICENAME`	Name to display on the user interface.	Required.
`DESCRIPTION`	Describe the service.	Required.
`ITDIURL`	Specify the URL for the Tivoli Directory Integrator instance. Valid syntax `isrmi://ip-address:port/ITDIDispatcher`, where `ip-address` is the Tivoli Directory Integrator host, and `port` is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`.	Required.
`SERVICEUID`	An identifier used to uniquely identify a user of an identity provider.	Required.
`TEST_CONNECTION`	Value `true` or `false`. Specify whether to test the connection before creating or updating the identity provider. If set to `true`, an identity provider is created or updated only if a connection test is successful. If `false`, the identity provider is created or updated without a connection test.	Optional. The default is set to **True**.

Attribute column header	Description	Required
URL	Specify the host name or IP address for the resource. For IPv6 addresses, enter the address value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`.	Optional.
POSIXRXATIMEOUTVALUE	Specify a value, in milliseconds, to control how long the adapter waits for a response after a remote command is issued to a managed resource. Modify this default if value operations on the managed resource timeout frequently.	Optional.
POSIXHOMEDIRREMOVE	Specify whether to delete the home directory of the user on the Solaris server when the account is deleted. Values: `true` or `false`.	Required.
POSIXRETURNSUDOPRIVILEGES	If `true`, the adapter returns the sudo privileges granted to users and groups during reconciliation. Values: `true` or `false`.	Optional.
POSIXSUDOERSPATH	If it is not the default location `/etc/sudoers` on the resource, enter the directory path to the `sudoers` file.	Optional.
OWNER	Specify the owner of the resource.	Optional.
POSIXUSESUDO	Specify whether the administrator has sudo capability on the Solaris server. Values: `true` or `false`.	Optional.
POSIXAUTHMETHOD	Select the authentication method. **Password Based Authentication** uses a password to authenticate users. **Key Based Authentication** requires the use of a passphrase and private key file to authenticate users.	Optional.
PASSWORD	A password used to authenticate a user.	Optional.
POSIXPASSPHRASE	Enter the passphrase to use for key based authentication. Required for key based authentication.	Optional.
POSIXPKFILE	Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.	Optional.
POSIXALFILESYSTEMPATH	Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Privileged Identity Manager. You can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles`. Alternatively, you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux operating system: system: `/opt/IBM/TDI/V7.1/profiles`.	Optional.
POSIXMAXCONNECTIONCNT	Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter `10` if you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter `0`, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.	Optional.
POSIXDISABLEALCACHE	Specify `true` to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.	Optional.

SOFTLAYER subtype:

Know about the identity provider column headers for bulk loading SOFTLAYER identity providers.

Attribute column header	Description	Required
`ORG_PDN`	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)` You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input. It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location `China`, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
`ORG_URI`	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
`IDENTITY_PROVIDER_PDN`	IDENTITY_PROVIDER_PDN is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for IDENTITY_PROVIDER_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`  You must specify an IDENTITY_PROVIDER_PDN which can uniquely identify an identity provider. If the specified IDENTITY_PROVIDER_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  For example:  `erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`  where `<idp attribute>=<value>,<full path of the admin domain>` **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
`SERVICENAME`	Name to display on the user interface.	Required.
`ITDIURL`	Specify the URL for the Tivoli Directory Integrator instance. Valid syntax `isrmi://ip-address:port/ITDIDispatcher`, where ip-address is the Tivoli Directory Integrator host, and port is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`.	Required.
`SOFTLAYERURL`	Specify the URL which the adapter can use to communicate with SoftLayer. For the current SoftLayer release, use `https://api.softlayer.com`.	Required.
`SOFTLAYERPIUSER`	Specify the user name of the user with the API key. Use the master account for full adapter functionality.	Required.
`SOFTLAYERAPIKEY`	Specify the API key for the user specified in the API User field.	Required.

Attribute column header	Description	Required
`TEST_CONNECTION`	Value `true` or `false`. Specify whether to test the connection before creating or updating the identity provider. If set to `true`, an identity provider is created or updated only if a connection test is successful. If `false`, the identity provider is created or updated without a connection test.	Optional. The default is set to **True**.
`SOFTLAYERSYNCVPNPASSWORD`	Boolean. Specify whether to synchronize the SoftLayer VPN password to the portal password. Values: `true` or `false`. When password synchronization is enabled: • The VPN password for the created accounts is set to be the same as the account (portal) password. The value specified for the VPN password in the account form is ignored. • Every time the account password is changed, the VPN password is also updated accordingly.	Optional.
`SOFTLAYERALFILESYSTEMPATH`	Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Privileged Identity Manager. You can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles`. Alternatively, you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux operating system: system: `/opt/IBM/TDI/V7.1/profiles`.	Optional.
`SOFTLAYERMAXCONNECTIONCNT`	Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter `10` if you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter `0`, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.	Optional.
`SOFTLAYERDISABLEALCACHE`	Specify `true` to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.	Optional.

`SQL2000` subtype:

Know about the identity provider column headers for bulk loading `SQL2000` identity providers.

Attribute column header	Description	Required
`ORG_PDN`	`ORG_PDN` is a query string for the system to search for qualified admin domains. 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.)`  You must specify an `ORG_PDN` which can uniquely identify an admin domain. If the specified `ORG_PDN` resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input.  It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location `China`, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`. You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required. See note. You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
`ORG_URI`	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either `ORG_URI` or `ORG_PDN` when you create an identity provider. Specifying these attributes is optional when you update the identity provider.

Attribute column header	Description	Required
`IDENTITY_PROVIDER_PDN`	`IDENTITY_PROVIDER_PDN` is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for `IDENTITY_PROVIDER_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`  You must specify an `IDENTITY_PROVIDER_PDN` which can uniquely identify an identity provider. If the specified `IDENTITY_PROVIDER_PDN` resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  For example: `erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`  where `<idp attribute>=<value>,<full path of the admin domain>` **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
`SERVICENAME`	Name to display on the user interface.	Required.
`DESCRIPTION`	Describe the service.	Required.
`URL`	URL of the data source. Supported protocols include: http, and https. This attribute is required.	Required.
`UID`	An identifier used to uniquely identify an identity provider.	Required.
`PASSWORD`	A password used to authenticate a user.	Required.
`SQL2000SERVERNAME`	Specify the instance name of SQL Server to be managed by this SQL Server Service. The instance name value is an IP address or host name.	Required.
`TEST_CONNECTION`	Value `true` or `false`. Specify whether to test the connection before creating or updating the identity provider. If set to `true`, an identity provider is created or updated only if a connection test is successful. If `false`, the identity provider is created or updated without a connection test.	Optional.
`SQL2000ADMINACCOUNT`	Specify the SQL Server instance administrator account name.	Optional.
`SERVICEPWD1`	Specify the SQL Server instance administrator account password.	Optional.
`SQL2000AUTHMETHOD`	Specify an authentication mode by which the adapter connects to the SQL Server. • `0` - With SQL Server authentication, the adapter uses the values from the SQL Admin Account and SQL Admin Password attributes for authentication. • `1` - With Windows authentication, the adapter uses the Windows account of the SQL Server Adapter windows service. The adapter uses the value from the **Log On As** attribute of the **SQL Server Adapter Windows service**. With Windows authentication, the adapter does not use the values from **SQL Admin Account** and **SQL Admin Password** attributes for authentication. `LocalSystem` is the default Windows account of a SQL Server Adapter Windows service after the adapter installation. Change the Log On account to a domain Windows account that is also a member of the sysadmin Server role in the SQL Server instance to which the adapter is connecting. For example, `DOMAIN\user`.	Optional.

Example 1 - adding an entry

```
#IdentityProviders,SQL2000
SERVICENAME,DESCRIPTION,URL,UID,PASSWORD,SQL2000SERVERNAME,ORG_PDN,
SQL2000ADMINACCOUNT,SERVICEPWD1
"SQL Server 187","SQL 2008R2 Server","http://192.0.2.10",agent,agent,192.0.2.12,
"ou=Valerie Workspace,ou=HR,l=China,o=IBM",sa,no_secret
```

Example 2 - updating an entry

```
#IdentityProviders,SQL2000
IDENTITY_PROVIDER_PDN,SERVICENAME,DESCRIPTION
"erservicename= SQL Server 187,ou=Valerie Workspace,ou=HR,l=China,o=IBM",
"SQL Server 187-rename","This is an update."
```

WINDOWS_LOCAL subtype:

Know about the identity provider column headers for bulk loading WINDOWS_LOCAL identity providers.

Attribute column header	Description	Required
ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. 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.)` You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results IBM Security Privileged Identity Manager treats it as invalid input. It is suggested that you use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location China, for organization IBM, use "ou=Valerie Workspace, ou=HR, l=China, o=IBM". You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements: `o=<Organization Name>` `l=<Location Name>` `ou=<Organization Unit>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
ORG_URI	Specify the organizational container under which the identity provider 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 are 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 an identity provider. Specifying these attributes is optional when you update the identity provider.	Required. See note. You must specify either ORG_URI or ORG_PDN when you create an identity provider. Specifying these attributes is optional when you update the identity provider.
IDENTITY_PROVIDER_PDN	IDENTITY_PROVIDER_PDN is a query string for the system to search for qualified identity providers. The following pseudo Backus-Naur Form (BNF) notation represents the syntax for IDENTITY_PROVIDER_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`  You must specify an IDENTITY_PROVIDER_PDN which can uniquely identify an identity provider. If the specified IDENTITY_PROVIDER_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  For example:  `erservicename=DB2 Service, ou=Valerie Workspace, ou=HR, l=China, o=IBM`  where `<idp attribute>=<value>,<full path of the admin domain>` **Note:** The values are space character-sensitive. Unnecessary spaces in the value may cause failure of PDN resolution.	Required only when you are updating an identity provider.
SERVICENAME	Name to display on the user interface.	Required.
ITDIURL	Specify the URL for the Tivoli Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where ip-address is the Tivoli Directory Integrator host, and port is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`.	Required.
DESCRIPTION	Describe the service.	Required.
URL	URL of the data source. Supported protocols include: http, and https. This attribute is required.	Required.
UID	An identifier used to uniquely identify an identity provider.	Required.

Attribute column header	Description	Required
PASSWORD	A password used to authenticate a user.	Required.
TEST_CONNECTION	Value true or false. Specify whether to test the connection before creating or updating the identity provider. If set to true, an identity provider is created or updated only if a connection test is successful. If false, the identity provider is created or updated without a connection test.	Optional.
WINLOCALSERVER	Specify the location of the remote server that you want to manage. If this parameter is NULL, the adapter uses the local computer.	Optional.
OWNER	Specify the owner of the resource.	Optional.
PREREQUISITE	Specify an IBM Security Privileged Identity Manager service that is prerequisite to this service.	Optional
URI	Identify the names of the resource.	Optional.

Example 1

```
#IdentityProviders,WINDOWS_LOCAL
SERVICENAME,DESCRIPTION,URL,UID,PASSWORD,ORG_PDN
"WinLocal 173","Windows Local Server 173","http://192.0.2.20",agent,agent,
"erglobalid=2427910216527938618,ou=orgChart,
erglobalid=00000000000000000000,ou=EXAMPLE,DC=COM"
```

Other identity provider subtypes

Learn how to bulk upload identity providers that are not part of the bundled identity providers.

Note: You cannot bulk upload **OpenSSHKeyProvider** identity provider.

Recognize the CSV file format that you want to create

The CSV file bulk load format is in the following form:

```
#IdentityProviders, <subtype>
<generic header1>, <generic header2>, <generic header3>, <property header1>,
<property header2>
<actual data>, <actual data>, <actual data>,<actual data>, <actual data>
```

<subtype>
> <subtype> is the adapter profile name that can be found in Service Center. In **Service Center**, click **Manage Identity Providers**, **All provider types**.

<generic header>
> This header is the same as the bundled identity providers. These are **ORG_PDN**, **ORG_URI**, **TEST_CONNECTION**, and **IDENTITY_PROVIDER_PDN**. See "#IdentityProviders type identifier column headers" on page 81.

<property header>
> This header is transformed from the attribute names of the LDAP object class of an identity provider. Those attribute names can be found in the identity provider form template file (xml format) in an adapter profile (jar file). For example, attributes for Linux adapters can be found in erPosixLinuxRMIService.xml of PosixLinuxProfile.jar. To get these headers, check the form templates that are saved under "ou=formTemplates,ou=itim,ou=*<your organization>*,DC=COM".

Converting the form templates to identify provider column headers

In the form template, take note of the formElement. The name is data.<ldap attribute name> for example "data.erservicename". The header is transformed from LDAP attributes by removing er if it is present. For example:

- erservicename becomes servicename
- owner remains as owner

If the `formElement` is read-only, do not use it as a CSV header.

Other conversions:

Control	Available values
Check box control	`TRUE` or `FALSE`
Select control	The available values are the option values.

Check the identity provider user interface to get an explanation of the expected value for each control.

#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.

Table 15.

Attribute for column header	Description	Required
`ACCOUNT_UID`	Specifies the user ID that is associated with the credential.	Required.
`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.	Required. 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`	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:
	
	`ou=Valerie Workspace`
	
	where ou=<admin domain name>
		Required.
		
		You must specify either `ORG_URI` or `ORG_PDN` when you create a credential. Specifying these attributes is optional when you update the credential.

`RESOURCE_UID`	Specifies the resource unique ID.	Required.
`RESET_PASSWORD`	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`.	Optional.
`PASSWORD`	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.	Optional.
`DESCRIPTION`	Provides a brief description about the credential that is added to the credential vault.	Optional.

Table 15. (continued)

Attribute for column header	Description	Required
`USE_DEFAULT_SETTINGS`	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 column headers (`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 column headers is specified, the credential will not use global default settings; the `USE_DEFAULT_SETTINGS` value is set to `FALSE`.	Optional.
`ACCESS_MODE`	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).	Optional.
`PASSWORD_VIEWABLE`	Specifies whether to display the credential password to users on the self-service user interface. The default value is `TRUE`.	Optional.
`MAX_CHECKOUT_DURATION`	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`.	Optional.
`ENABLE_CHECKOUT_SEARCH`	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`.	Optional.
`RESET_PASSWORD_ON_CHECKIN`	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.	Optional.
`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, credentials are created but not connected. If you specify a blank value for this column, the credential is not connected. 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: `erservicename=winlocalService,ou=Valerie Workspace`  where `<idp attribute>=<value>,ou=<admin domain name>`	Optional.
`DISCONNECT`	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.	Optional.

Table 15. (continued)

Attribute for column header	Description	Required
`CREDENTIAL_TAG`	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.	Optional.
`PASSWORD_ROTATION_INTERVAL`	Optional. Specifies the number days before IBM Security Privileged Identity Manager resets the password. The value must be an integer. This parameter applies only when the credential is connected to an identity provider. For example: 5.	Optional.

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
vicgreen,"ou=Finance,o=Organization",not_secret,vic.example.com
```

In this example, the credential (user ID `vicgreen`, password `not_secret`) is added to the credential vault. The `RESOURCE_UID` is a URL, `vic.example.com`. Global credential settings are used. Other than the password and the resource name, only the required attributes are specified. The password must be rotated after 5 days.

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,ORG_PDN,PASSWORD_VIEWABLE
vicgreen,vic.example.com,
"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`) 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,
CREDENTIAL_SERVICE,CONNECT_SERVICE_PDN,PASSWORD_ROTATION_INTERVAL
vicgreen,"ou=Finance,o=Organization",not_secret,vic.example.com,
Vic's Linux Service,Vic_Linux|VicGreen_Linux,"description=winlocalService,
l=San Francisco,ou=Admin,o=ibm",5
```

In this example, credential (user ID `vicgreen`, password `not_secret`) is added as a credential that is connected to a service with pseudo DN of `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.

#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.

You can only bulk upload credential pools for password credentials.

Attribute for column header	Description	Required
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.	Required for modifying an existing credential pool.
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.	Required.
RESOURCE_UID	Specifies the resource unique ID.	Required.
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.	Required.
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.	Required. You must specify either ORG_URI or ORG_PDNwhen you create a credential. Specifying these attributes is optional when you update the credential.

Attribute for column header	Description	Required
`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.	Required.
`DESCRIPTION`	Provides a brief description about the credential pool that must be added to the credential vault.	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_v2
POOL_NAME,RESOURCE_UID,POOL_RULE,ORG_PDN,DESCRIPTION
ITIMPool,vic.samplecompany.com,"tag1|tag2",
"ou=HR Department","ITIM Pool Description"
```

Sample CSV file for modifying the credential pool

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

```
#CredentialPools_v2
POOL_PDN,POOL_RULE,ORG_PDN,
"description=testpool,l=Pune,ou=Finance,o=Organization",
"Guests|Helpdesk","ou=Finance",
```

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

#Access type identifier column headers
The **#Access** type identifier allows you to handle bulk uploads of accesses. This page lists the #Access type identifier column headers in a shared access comma-separated value (CSV) file.

#Access

See the following tables that describe the columns that you can define in the CSV file:

Attribute column headers	Description	Requirement for creating a new access	Requirement for updating an access	Remarks
ORG_PDN	ORG_PDN is a query string for the system to search for qualified admin domains. The following pseudo BNF notation represents the syntax for ORG_PDN: `<div style="background-color:lightgray;"> <pre>orgDn ::= orgRdn	orgRdn "," orgDn orgRdn ::= orgAttr '=' value orgAttr::= string (Must be a valid attribute name of the organizational container.)</pre></div>`  You must specify an ORG_PDN which can uniquely identify an admin domain. If the specified ORG_PDN resolves to multiple results, IBM Security Privileged Identity Manager treats it as invalid input.  You can use the full path of the admin domain. For example, if you have an admin domain named `Valerie Workspace` that belongs to the Organization Unit HR, with location China, for organization IBM, use `"ou=Valerie Workspace, ou=HR, l=China, o=IBM"`.  You can find the admin domain name in the top left corner of the Service Center. The rest of the pseudo DN is the path of the admin domain. In the path, you can use the following elements:  `<div style="background-color:lightgray;"> <pre>o=<Organization Name> l=<Location Name> ou=<Organization Unit></pre></div>` You can find the path of an admin domain in the administrative console, under **Manage Organization Structure**.	Required	Not required	-
ACCESS_PDN	ACCESS_PDN is a query string for the system to search for qualified resources. The following BNF notation represents the syntax for ACCESS_PDN: `accessPDN ::= access-name = string, orgDN orgDN ::=orgRdn orgRdn "," orgDn orgRdn ::=orgAttr'=' value orgAttr::=string` You must specify an ACCESS_PDN which can uniquely identify an access. If the specified ACCESS_PDN lists multiple results, IBM Security Privileged Identity Manager treats it as invalid input.	Not required	Required	-
ACCESS_NAME	Specifies the access name.	Required	Optional	-
ACCESS_DESCRIPTION	Specifies a brief description.	Optional	Optional	-
ACCESS_ASSIGNMENT_TYPE	Specifies one of the following assignment types: • **byRequest**: Users can request access, which can then be granted according to the approval workflow. The access owner can also grant access to users. • **byOwner**: The access owner grants access to users. • **byRule**: Users that match an LDAP search filter are automatically granted access.	Required	Not required	Valid values: • **byRequest** • **byOwner** • **byRule** – Case sensitive
ACCESS_ADDITIONAL_INFO	Specifies the value that is only valid for the **byRequest** assignment type. **Note:** This value also provides additional information for the access. It is only valid for **byRequest**.	Optional	Optional	-
ACCESS_APPROVAL_WORKFLOW	Specifies the name of the access request workflow. This value is only valid for byRequest type. **Note:** This value must have the same name of the configured Access Approval Workflows. Note:	Optional for **byRequest**	Optional for **byRequest**	Do not use this header or specify an empty value for other assignment types. For example, **byOwner** or **byRule**.

Attribute column headers	Description	Requirement for creating a new access	Requirement for updating an access	Remarks
RULE	Specifies an LDAP filter. The users that match this filter are automatically granted access. For example: (**uid=admin***)	Optional for **byRule**	Optional for **byRule**	Do not use this header or specify an empty value for other assignment types. For example, **byOwner** or **byRequest**.

Members

Note: If you are updating an access and this header is defined in the CSV file, all members in the current access are reset.

Attribute column headers	Description	Requirement for creating a new access	Requirement for updating an access	Remarks
LOGIN_ID	Specifies the user login ID. For example, Valerie.	Required	Required	-

Entitlements

Note: If you are updating an access and this header is defined in the CSV file, all entitlements in the current access are reset.

Attribute column headers	Description	Requirement for creating a new access	Requirement for updating an access	Remarks
ENTITLEMENT_TYPE	Specifies one of the following entitlement types: **credential** Specifies entitlements for a set of credentials. **credentialPool** Specifies 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 includes newly added credentials or credential pools that match the filter.	Required	Required	Valid values: • **filter** • **credential** • **credentialPool**- Case sensitive
CREDENTIAL_OR_POOL_NAME	Specifies the login ID of the credential, or the name of the credential pool.	Required for **credential** and **credentialPool**	Required for **credential** and **credentialPool**	Do not use this header or specify an empty value for the filter type.
CREDENTIAL_TYPE	Specifies the credential authenticator type: password or sshkey	Optional	Optional	If not specified, this attribute defaults to password. This is only applicable to the **credential** entitlement type.
RESOURCE_UID	Specifies the resource unique ID.	Required for **credential** and **credentialPool**	Required for **credential** and **credentialPool**	Do not use this header or specify an empty value for the filter type.
FILTER_NAME	Specifies the filter name.	Required for **filter**	Required for **filter**	-

Attribute column headers	Description	Requirement for creating a new access	Requirement for updating an access	Remarks
FILTER_TYPE	Specifies one of the following filter types: • **credential** • **credentialPool**- Case sensitive	Required for **filter**	Required for **filter**	-
CREDENTIAL_OR_POOL_NAME_CRITERION	The filtering criterion only supports exact match and start with match. For example: Enter abc for the exact match of the string, abc* for a string starting with abc, abc1, and abc2.	Optional for **filter**	Optional for **filter**	When there are no values specified for CREDENTIAL_OR_POOL_NAME_CRITERION, RESOURCE_NAME_CRITERION, RESOURCE_TAG_CRITERION), it means "Include All".
RESOURCE_NAME_CRITERION	The filtering criterion only supports exact match and start with match. For example: Enter abc for the exact match of the string, abc* for a string starting with abc, abc1, and abc2.	Optional for **filter**	Optional for **filter**	-
RESOURCE_TAG_CRITERION	The filtering criterion only supports exact match and start with match. For example: Enter abc for the exact match of the string, abc* for a string starting with abc, abc1, and abc2.	Optional for **filter**	Optional for **filter**	-

The following sample CSV file contains information about granting and modifying accesses:

Sample CSV file for granting access **byRequest**

```
#Access
ACCESS_NAME,ACCESS_ASSIGNMENT_TYPE,ORG_PDN,RULE, ACCESS_DESCRIPTION,
ACCESS_APPROVAL_WORKFLOW access to build servers, byRequest,"ou=Vic Workspace,
o=2046",, grant support team to access build servers,  Access Request Workflow 1
##Entitlement
ENTITLEMENT_TYPE, CREDENTIAL_OR_POOL_NAME, CREDENTIAL_TYPE, RESOURCE_UID
credential, db2admin1, SSH_KEY, proddb1
credentialPool,Credential Pool proddb2, proddb2
##Entitlement
ENTITLEMENT_TYPE, FILTER_NAME, FILTER_TYPE, CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION, RESOURCE_TAG_CRITERION
filter, pool_filter, credentialPool, admin*, redhat*,
##Members
LOGIN_ID
vic
amy
barbara
```

Sample CSV file for granting access **byOwner**

```
#Access
ACCESS_NAME,ACCESS_ASSIGNMENT_TYPE,ORG_PDN,RULE, ACCESS_DESCRIPTION
access to bvt test servers, byOwner,"ou=Vic Workspace, o=2046",,grant support
team to bvt servers,
##Entitlement
ENTITLEMENT_TYPE, CREDENTIAL_OR_POOL_NAME, RESOURCE_UID
credential,db2admin1, proddb1
credentialPool,Credential Pool proddb2, proddb2
##Members
LOGIN_ID
vic
amy
barbara
```

Sample CSV file for modifying an access

```
#Access
ACCESS_PDN,ACCESS_NAME, ACCESS_DESCRIPTION, ACCESS_ADDITIONAL_INFO,
ACCESS_APPROVAL_WORKFLOW "access-name = access to build servers, ou=Vic Workspace,
o=2046", modify-name, modify-description, modify-info,Access Request Workflow 2
##Entitlement
ENTITLEMENT_TYPE, FILTER_NAME, FILTER_TYPE, CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION, RESOURCE_TAG_CRITERION filter,
All Credential Pool, credentialPool,,,
```

#ManagedInstances type identifier column headers

Use the #ManagedInstances type identifier to handle bulk upload of application services.

Important: Managed application services can only be bulk uploaded through Service Center.

The following list describes the type identifier column headers that you can use.

Attribute column header	Description	Required
MANAGED_SERVICE_NAME	Specifies the common name that is used for the managed application service.	Required.
HOST	Specifies the host of the managed application service.	Required.
TARGET_UNIQUE_NAME	Specifies the short name that associated with the service. This name must match the service name of the Windows service.	Required.
TARGET_DISPLAY_NAME	Specifies the displayed name associated with the service. This field is a descriptive name for the service.	Required.
CREDENTIAL_RESOURCE_UID	Identifies the UID of the resource that is associated with the managed application service.	Optional.
NOTIFY_EMAIL	Specify recipients of the notification email. Separate multiple recipients with a comma (,), enclosing recipients in double quotes (""). Notifications will always be sent to the person who registered the service manager regardless of whether the field is populated or not. For example: "abc@example.com,def@example.com"	Optional.
RESTART	Specifies whether to restart the service after a reconfiguration. Acceptable values are true or false. If true, the service is restarted after configuration.	Optional.
MANAGED_SERVICE_TYPE	Specifies the type of service that you are managing. The types are windows-service for Windows services and windows-scheduled-task for Windows scheduled tasks. The default value is windows-service.	Optional.
CREDENTIAL_USER_NAME	Specifies the credential that is associated with the managed application service. **Note:** This only matches for password credentials.	Optional.
ACTIVE	Specifies whether the service is managed by the service management agent. Acceptable values are true or false. If set to true, the service managed by the agent. If set to false, the service is not managed. Default value: true	Optional.

Each CSV entry represents one managed application service instance. If the managed application service instance does not exist, the application service is created. If an application service exists, the application service is updated.

The system uses the **HOST** and **TARGET_UNIQUE_NAME** to determine if an application service instance exists.

Example 1

The following sample CSV file contains information about the managed application services:

```
#ManagedInstances
MANAGED_SERVICE_NAME,HOST,TARGET_UNIQUE_NAME,TARGET_DISPLAY_NAME,
NOTIFY_EMAIL,RESTART,
MANAGED_SERVICE_TYPE,CREDENTIAL_USER_NAME,CREDENTIAL_RESOURCE_UID,ACTIVE
DB2 - DB2COPY1 - DB2-0,192.0.2.5,DB2-0,DB2 - DB2COPY1 - DB2-0,,false,
windows-service,user1,IBM-PK06KHY,true
```

In this example, the Windows service (DB2 - DB2COPY1 - DB2-0) is added.

If `HOST` and `TARGET_UNIQUE_NAME` already exists in the system, the existing application service will be updated.

The CSV file column headers are an unordered list. You can change the order of these column headers. However, do not change the name of these column headers.

The uploaded service belongs to the current Admin domain and are assigned to the current application manager of the bulk upload session.

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.

Credential bulk upload

You can bulk upload credentials in the same CSV file.

If you are specifying related credentials in the same CSV file, use the `#Credentials_v2` type identifier format. For more information, see "#Credentials_v2 type identifier column headers" on page 99. The **ACCESS_MODE** must be set to 1.

Example 2 - Specifying managed instances with credentials in the same CSV file

```
#Credentials_v2
ACCOUNT_UID,PASSWORD,ACCESS_MODE,RESOURCE_UID
user1, secret, 1, PIMQA

#ManagedInstances
MANAGED_SERVICE_NAME,HOST,TARGET_UNIQUE_NAME,TARGET_DISPLAY_NAME,
NOTIFY_EMAIL,RESTART,MANAGED_SERVICE_TYPE,CREDENTIAL_USER_NAME,
CREDENTIAL_RESOURCE_UID,ACTIVE
DB2 - DB2COPY1 - DB2-0,192.0.2.5,DB2-0,DB2 - DB2COPY1 - DB2-0,,false,
windows-service,
user1,PIMQA,true
```

Application service instance matching for the `#ManagedInstances` type:

Each CSV entry represents one managed application service instance. If the managed application service instance does not exist, the application service is created. If an application service exists and the specified application service configuration is different, the application service is updated.

Example CSV file with credentials and identity providers

See an example of a CSV file for bulk loading of both credentials and identity providers.

```
#Resources
ORG_PDN,RESOURCE_NAME,RESOURCE_UID
ou=IBM,"identity upload",1783157521045806653

#Resources
ORG_PDN,RESOURCE_NAME,RESOURCE_UID,RESOURCE_ALIAS
ou=IBM,"Solaris Mock 97",1068345022549246195,10.167.13.97
```

```
ou=IBM,"AIX Mock 97",1067763381389137791,10.127.13.95
ou=IBM,"WindowAD service 88",1065675348461381568,http://10.187.3.88
ou=IBM,"Linux Service 69",1267256030380649897,10.127.13.69
ou=IBM,"Linux Service 87",1067000233873787420,10.127.13.87
ou=IBM,S209,1790829810611227446,10.187.3.209
ou=IBM,"Ldap Mock 93",1067378791952312307,ldap://localhost:389
ou=IBM,linux69,linux69,,10.127.13.16
ou=IBM,"Linux Service 69",10.127.13.69,,

#IdentityProviders,PosixSolarisProfile
ORG_PDN,SERVICENAME,URL,POSIXDISABLEALCACHE,SERVICEUID,POSIXSUDOERSPATH,ITDIURL,
POSIXRETURNSUDOPRIVILEGES,POSIXHOMEDIRREMOVE,POSIXUSESUDO,POSIXAUTHMETHOD,TEST_CONNECTION
ou=IBM,"Solaris Mock 97",10.167.13.97,false,admin,/etc/sudoers,
rmi://localhost:1099/ITDIDispatcher,false,false,false,pba,false

#IdentityProviders,PosixAixProfile
ORG_PDN,SERVICENAME,OWNER,URL,AUTHENTICATEMODE,POSIXDISABLEALCACHE,POSIXSUDOERSPATH,
POSIXHOMEDIRREMOVE,SERVICEUID,ITDIURL,
POSIXRETURNSUDOPRIVILEGES,POSIXUSESUDO,POSIXAUTHMETHOD,TEST_CONNECTION
ou=IBM,"AIX Mock 97",uid=jill,10.127.13.95,0,false,/etc/sudoers,true,admin,
rmi://localhost:1099/ITDIDispatcher,true,true,pba,false

#IdentityProviders,ADprofile
ORG_PDN,SERVICENAME,PASSWORD,URL,UID,TEST_CONNECTION
ou=IBM,"WindowAD service 88",agent,http://10.187.3.88,agent,false

#IdentityProviders,PosixLinuxProfile
ORG_PDN,SERVICENAME,OWNER,URL,AUTHENTICATEMODE,POSIXDISABLEALCACHE,POSIXSUDOERSPATH,
POSIXHOMEDIRREMOVE,SERVICEUID,POSIXUSESHADOW,ITDIURL,
POSIXRETURNSUDOPRIVILEGES,POSIXUSESUDO,POSIXAUTHMETHOD,TEST_CONNECTION
ou=IBM,"Linux Service 69",uid=tuser1,10.127.13.69,0,false,/etc/sudoers,false,root,true,
rmi://localhost:1099/ITDIDispatcher,false,false,pba,false

#IdentityProviders,PosixHpuxProfile
ORG_PDN,SERVICENAME,URL,POSIXDISABLEALCACHE,POSIXSUDOERSPATH,POSIXHOMEDIRREMOVE,
POSIXEXECUTEUSERPROFILE,SERVICEUID,POSIXUSESHADOW,ITDIURL,
POSIXRETURNSUDOPRIVILEGES,POSIXUSESUDO,POSIXAUTHMETHOD,TEST_CONNECTION
ou=IBM,"HP-UX Mock 98",10.167.13.98,false,/etc/sudoers,true,false,admin,true,
rmi://localhost:1099/ITDIDispatcher,true,false,pba,false

#IdentityProviders,PosixLinuxProfile
ORG_PDN,SERVICENAME,PASSWORD,URL,AUTHENTICATEMODE,POSIXPASSPHRASE,POSIXDISABLEALCACHE,
POSIXSUDOERSPATH,POSIXHOMEDIRREMOVE,SERVICEUID,POSIXUSESHADOW,ITDIURL,
POSIXRETURNSUDOPRIVILEGES,POSIXUSESUDO,POSIXAUTHMETHOD,TEST_CONNECTION
ou=IBM,"Linux Service 87",p@ssw0rd,10.127.13.87,0,p@ssw0rd,false,/etc/sudoers,false,root,true,
rmi://localhost:1099/ITDIDispatcher,false,true,kba,false

#IdentityProviders,PosixLinuxProfile
ORG_PDN,SERVICENAME,PASSWORD,URL,AUTHENTICATEMODE,POSIXDISABLEALCACHE,POSIXSUDOERSPATH,
POSIXHOMEDIRREMOVE,SERVICEUID,POSIXUSESHADOW,ITDIURL,POSIXRETURNSUDOPRIVILEGES,POSIXUSESUDO,POSIXAUTHMETHOD,
TEST_CONNECTION
ou=IBM,S209,p@ssw0rd,10.187.3.209,0,false,/etc/sudoers,false,root,true,
rmi://localhost:1099/ITDIDispatcher,false,false,pba,false

#IdentityProviders,LdapProfile
ORG_PDN,SERVICENAME,PASSWORD,AUTHENTICATEMODE,LDAPINITIALGRPMEM,DSNAME,LDAPGRPRDN,
USERCONTAINERDN,LDAPGRPMEMATTR,URL,LDAPDISABLEALCACHE,LDAPPAGESIZE,SERVICEUID,
GROUPSCONTAINERDN,LDAPGROUPCLASS,ITDIURL,LDAPUSESSL,LDAPUSERRDN,TEST_CONNECTION
ou=IBM,"Ldap Mock 93",admin,0,"cn=TIM Adapter",IDS,cn,cn=root,member,
ldap://localhost:389,false,15,admin,group=root,groupOfNames,
rmi://localhost:1099/ITDIDispatcher,true,true,UID,false

#Credentials_v2
ACCOUNT_UID,ORG_PDN,PASSWORD,USE_DEFAULT_SETTINGS,ACCESS_MODE,PASSWORD_VIEWABLE,
MAX_CHECKOUT_DURATION,ENABLE_CHECKOUT_SEARCH,RESET_PASSWORD_ON_CHECKIN,RESOURCE_UID
admin1,ou=IBM,p@ssw0rd,true,0,true,8h,true,true,linux69
admin2,ou=IBM,p@ssw0rd,false,0,true,6h,false,false,linux69
admin3,ou=IBM,test,false,1,true,true,9.127.13.69
admin4,ou=IBM,test,false,2,true,9.127.13.69

#Credentials_v2
ACCOUNT_UID,ORG_PDN,PASSWORD,USE_DEFAULT_SETTINGS,ACCESS_MODE,PASSWORD_VIEWABLE,
MAX_CHECKOUT_DURATION,ENABLE_CHECKOUT_SEARCH,RESET_PASSWORD_ON_CHECKIN,CONNECT_SERVICE_PDN,
RESOURCE_UID,CREDENTIAL_TAG
account1,ou=IBM,password,false,0,false,8h,true,true,"erServiceName=Linux Service 69,ou=IBM",
1267256030380649897,TestPool_1267256030380649897

#CredentialPools_v2
POOL_NAME,RESOURCE_UID,POOL_RULE,ORG_PDN
test,1267256030380649897,test_1267256030380649897,ou=IBM
test2,1267256030380649897,test2_1267256030380649897,ou=IBM
test3,1065675348461381568,test3_1065675348461381568,ou=IBM

#Access
ORG_PDN,ACCESS_NAME,ACCESS_ASSIGNMENT_TYPE
ou=IBM,ICEAdminRole,byRequest
##Members
LOGIN_ID
apark
buck
#Access
```

```
ORG_PDN,ACCESS_NAME,ACCESS_ASSIGNMENT_TYPE,ACCESS_ADDITIONAL_INFO
ou=IBM,static_role_by_request,byRequest,"additional info"
##Members
LOGIN_ID
cap
buck
someID
#Access
ORG_PDN,ACCESS_NAME,ACCESS_ASSIGNMENT_TYPE,RULE
ou=IBM,dynamic_role_1,byRule,(uid=test)
##Entitlement
ENTITLEMENT_TYPE,CREDENTIAL_OR_POOL_NAME,RESOURCE_UID
credential,account10,1267256030380649897
##Entitlement
ENTITLEMENT_TYPE,FILTER_NAME,FILTER_TYPE,CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION,RESOURCE_TAG_CRITERION
filter,filter,credential,account,name*,tag*
##Entitlement
ENTITLEMENT_TYPE,FILTER_NAME,FILTER_TYPE,CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION,RESOURCE_TAG_CRITERION
filter,ALL_CREDENTIALS_ENTITLEMENT,credential,,,
##Entitlement
ENTITLEMENT_TYPE,CREDENTIAL_OR_POOL_NAME,RESOURCE_UID
credential,account100,1267256030380649897
##Entitlement
ENTITLEMENT_TYPE,CREDENTIAL_OR_POOL_NAME,RESOURCE_UID
credential,account1,1267256030380649897
##Entitlement
ENTITLEMENT_TYPE,FILTER_NAME,FILTER_TYPE,CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION,RESOURCE_TAG_CRITERION
filter,ALL_CREDENTIAL_POOLS_ENTITLEMENT,credentialPool,,,
#Access
ORG_PDN,ACCESS_NAME,ACCESS_ASSIGNMENT_TYPE
ou=IBM,static_role_byowner,byOwner
##Members
LOGIN_ID
someID
#Access
ORG_PDN,ACCESS_NAME,ACCESS_DESCRIPTION,ACCESS_ASSIGNMENT_TYPE
ou=IBM,static_role_child,description,byRequest
##Members
LOGIN_ID
buck
##Entitlement
ENTITLEMENT_TYPE,FILTER_NAME,FILTER_TYPE,CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION,RESOURCE_TAG_CRITERION
filter,filter,credential,account,name*,tag*
##Entitlement
ENTITLEMENT_TYPE,FILTER_NAME,FILTER_TYPE,CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION,RESOURCE_TAG_CRITERION
filter,ALL_CREDENTIALS_ENTITLEMENT,credential,,,
##Entitlement
ENTITLEMENT_TYPE,FILTER_NAME,FILTER_TYPE,CREDENTIAL_OR_POOL_NAME_CRITERION,
RESOURCE_NAME_CRITERION,RESOURCE_TAG_CRITERION
filter,ALL_CREDENTIAL_POOLS_ENTITLEMENT,credentialPool,,,
```

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.

Uploading a CSV file with the administrative console

As a privileged administrator, you can add or update the credentials, credential pools, and identity providers, that are specified in the comma-separated value (CSV) file with the administrative console. You cannot upload managed instances 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, identity providers, or credential pools. If there is no setting change for a credential, identity provider, or credential pool, that entry is skipped.

If you are uploading a CSV file with defined managed instances, use the Service Center instead. See "Uploading a CSV file for application services with Service Center" on page 146.

Procedure

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 entities that are specified in the CSV file.

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 entities that are added, modified, or failed because of incorrect values in the CSV file.

Configuring the credential default settings

As a System Administrator you can specify the default settings for each credential that is added to the credential vault.

About this task

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.

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 or key upon check in
Select the check box to change the password or SSH Key when a credential is checked in.

Note: For credentials that are not connected to an account, the credential password or SSH Key is not changed at check-in even if **Change password or key upon check in** 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 in the self-service console.

Specify whether the credential password or key is visible to the user in Self Service User Interface
Select the **Allow view password or key download to user** check box to display the credential password or SSH Key to the user in the self-service user interface.

Check Out Operation
In the **Operation Name** field, enter a global lifecycle operation name that defines the check-out workflow extension.

Lease Expiration Handling

Notify violation
Select this option to send a notification when the system finds that the lease of a checked out credential has expired.

Notify violation and check in
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 lease 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.

Send notifications at least every
Schedule a time frequency to send out notifications to remind the recipients of the expired 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.

Do not require the check-in and check-out process for shared IDs
> Select this option to specify that, by default, users do not need to check out a shared credential before they use it.

> **Specify whether the credential password or key is visible to the user in Self Service User Interface**
>> Select the **Allow view password or key download to user** check box if you want to display the credential password or SSH Key to the user in the self-service user interface.

Credential is not shared
> Select this option if you do not want any user to access the credential. When you select this option, the credential is stored in the credential vault. However, the credential cannot be added into any access entitlements. Use this setting for SSH Key credentials that are only used for identity provider administrator authorization or forwarder authorization.

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

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**. You are prompted to open the Java Web start file.
2. Open the file with the Java Web Start Launcher and click **OK**.
3. In the left pane of the Design Form window, double-click the **Credential Lease** folder.
4. Double-click the **Credential Lease** form to open it in the form designer.
5. From the **Attribute List**, select one of the available custom attributes and click the **Add Row** icon to add it to the form.
6. Select one of the attributes from the **Credential Lease** form to customize the selected attribute with format and constraint properties.

   Note: Additionally, right click on the selected attribute and click **Change to** to change the behavior of the attribute.
7. Click the **Save Form Template** icon to save the changes and click **OK**.

Configuring the shared access credential usage prompt for Privileged Access Agent

As a System Administrator, you can 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" on page 176.

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 16. Password entry options

Password entry	Description
Automatic logon	Use only shared credentials to log on to the managed resources.
Always	Always asks the user whether to use shared credentials to log on.
Ask	Asks the user whether to use shared credentials to log on.
Never	Do not use shared credentials to log on to the managed resources.

Configuring the reauthentication prompt

For more security, IBM Security Privileged Identity Manager users can be asked to re-authenticate when they access managed resources. Configure whether to require the users to re-authenticate every time that a user accesses a client application or command that requires shared credentials.

Procedure

1. Start the Single Sign-On administration console.
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. Session recording administration

The IBM Privileged Session Recorder captures user activity of sessions on managed workstations.

Recording policies

As a session recording auditor, you can use AccessAdmin or the Administrative console to customize recording settings. You can customize settings such as recording quality, and keylogging enforcement.

Use AccessAdmin to configure the privileged session recording policies for connections that use the Privileged Access Agent client. You can customize settings such as recording quality and keylogging enforcement. See Policies for Privileged Access Agent.

Use the administrative console to configure the recording policies for sessions that are launched by using the Privileged Session Gateway. See "Configuring a session recording policy" on page 173

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 17. What you can search for in recordings

What you can search for	Text-based recordings	Screen-based recordings
General Search capabilities		
	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	(Privileged Access Agent) The Windows user who logged on to the client computer. (Privileged Session Gateway) The expected value is **N/A**.	
Application User ID	The credential name.	
Local host	Host name of the client computer. (Privileged Access Agent on a gateway) Terminal server or Remote Desktop Services gateway IP address. (Privileged Session Gateway) Client computer IP address where the browser is launched.	
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. (Privileged Session Gateway) The process name is **Privileged Session Gateway**.	
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 Session Recording Auditors.

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:

```
https://pimva.example.com/recorder/ui/SessionRecordingContainer.html?
recordingID=bba18928854e403ca5d619fdf709cda6
```

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 partition set" on page 122.

About this task

The following playback controls are available when you view recordings.
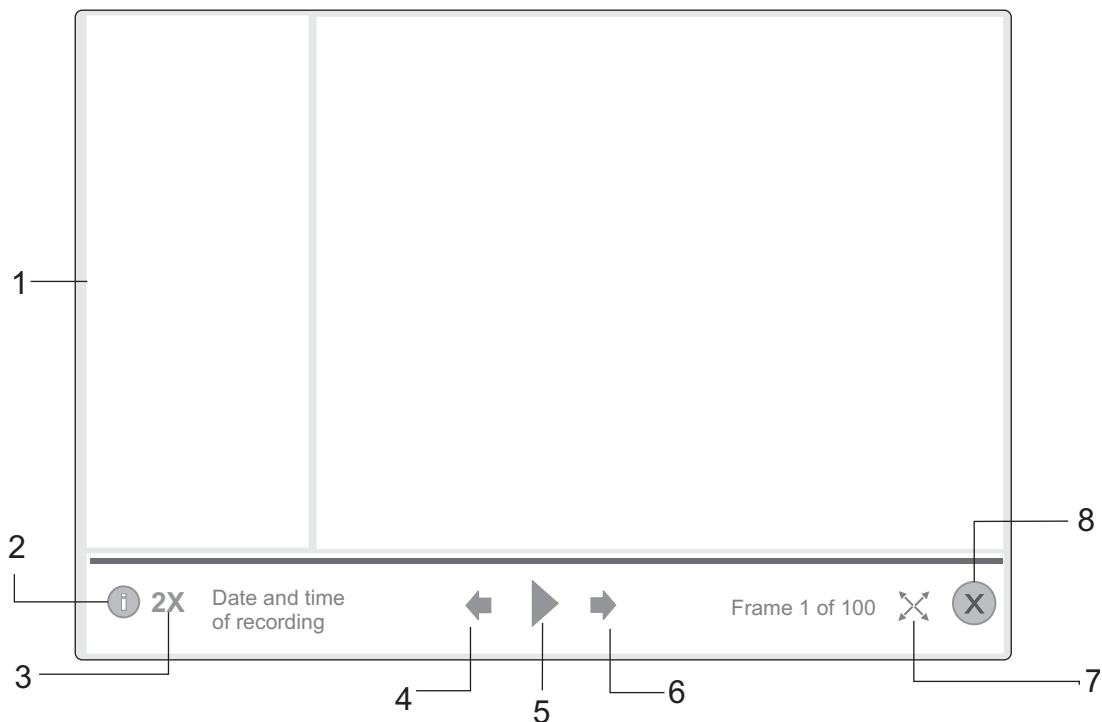
Figure 2. Playback and view controls

Table 18. 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.
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.

Checking existing partition sets

Check on existing partition sets in the current database and when it expires.

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 by executing the following command:

   `db2 describe data partitions for table recording`

Archiving a partition set

Archive partition sets to reduce the size of the Privileged Session Recorder database

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 by executing the following command:

   `db2 describe data partitions for table recording`

   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.

   Note: Ensure that you have the following files before proceeding to the next step.

```
-------------------------------
-- Files in the <archive_dir> --
-------------------------------
archiveInfo_<part_alias>
<part_alias>_BMARK_FILE
<part_alias>_FRAME_FILE
<part_alias>_FRFILE_FILE
```

```
<part_alias>_REC_FILE
<part_alias>_RECMD_FILE
./Frames
./Images


----------------------------------
-- Files in the ./Frames Folder --
----------------------------------
./Frames:
<part_alias>_FRAME_FILE.<number>.lob


----------------------------------
-- Files in the ./Images Folder --
----------------------------------
./Images:
<part_alias>_FRFILE_FILE.<number>.lob
```

For example:

```
archiveInfo_ARCHJUL2017
ARCHJUL2017_BMARK_FILE
ARCHJUL2017_FRAME_FILE
ARCHJUL2017_FRFILE_FILE
ARCHJUL2017_REC_FILE
ARCHJUL2017_RECMD_FILE
./Frames
./Images

./Frames:
ARCHJUL2017_FRAME_FILE.001.lob

./Images:
ARCHJUL2017_FRFILE_FILE.001.lob
```

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')
      ```

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 methods:
   - **call sp_create_partitionset('EXECUTE', n)**
   - **call sp_create_partitionset('EXECUTE', 1, '<part_name>')**

   Note:
   - Each method creates a new partition with a duration of n months.
   - When Privileged Session Recorder is activated, 12 partitions are created. Each partition has a duration of one month.
   - New partitions must be created by the user before the current partition set expires.

Restoring an archived partition set

Restore an archived partition set to retrieve a recording that is not found in the current database.

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')
```

Chapter 8. Application identity management

Application administrators can use Privileged Identity Manager for Applications (App ID) to remove hardcoded and unsafely stored credentials from applications, Windows services, and scripts. App ID can also be used to manage the credential entitlements, 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.
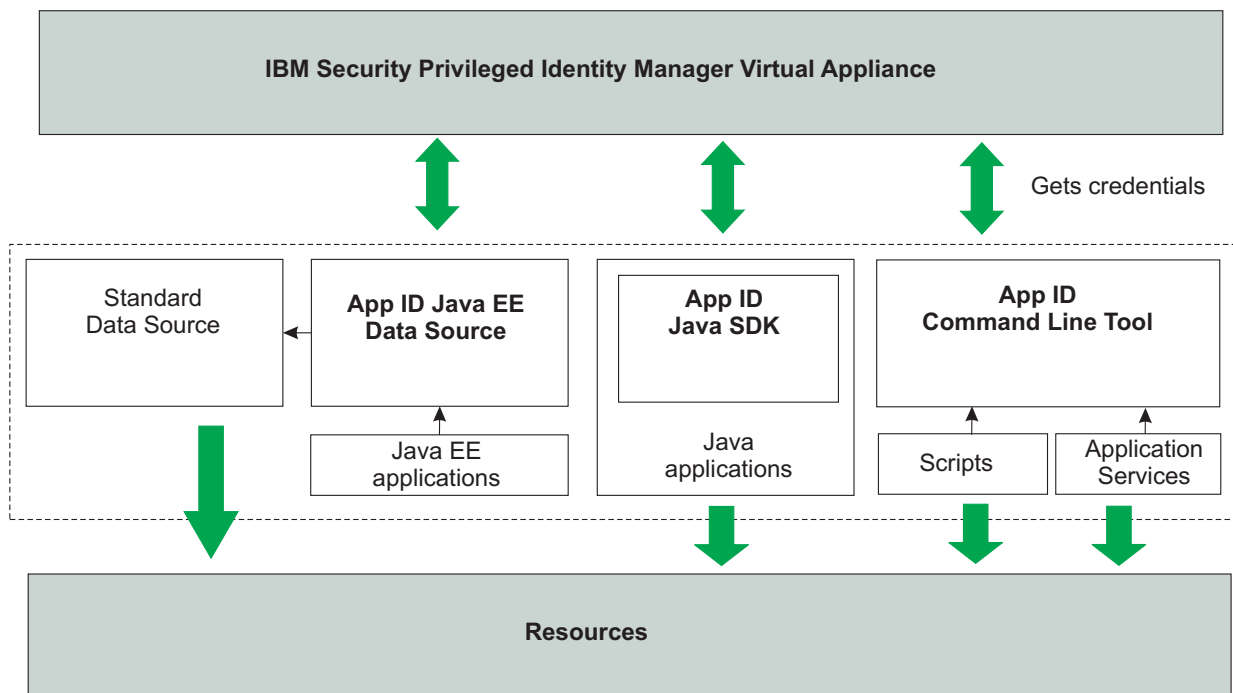
Figure 3. Credentials are often embedded inside data sources, custom applications, application services, or unattended scripts to retrieve sensitive information.

Application identity management helps application and IT administrators accomplish the following goals:

- Remove hard-coded and unsafely stored passwords from applications, scripts, Windows services, Windows Task Scheduler tasks, and their configuration files.
- Automatically change or rotate 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.

For application services, a service management agent can reconfigure managed application services with changed credentials. Types of application services include Windows services and Task Scheduler tasks.

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 are 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.

Note: All types of instances can only use password credentials.

The following steps describe the general process of enrolling a new application or application service to use managed credentials.

Table 19. Process of enrolling a new application or application service

Enrolling new	Steps

Applications
 	
Java EE data sources, Java applications, scripts
	1. Add the application credentials to the vault.
	  • Credentials for applications must be set to not require check-out. See "Specifying non-exclusive shared access credentials" on page 58.
	  • Configure a password rotation interval for credentials. See "Configuring a reset interval for credentials" on page 57.
	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 that it requires.

Table 19. Process of enrolling a new application or application service (continued)

Enrolling new	Steps

Application services
 	
Windows services, Windows Task Scheduler tasks
	1. Add the application credentials to the vault.
	  • Configure credentials to not require check-out. See "Specifying non-exclusive shared access credentials" on page 58.
	  • Configure a password rotation interval for credentials. See "Configuring a reset interval for credentials" on page 57.
	2. If not already done, set up a service management agent on a computer.
	  A service management agent can update configurations of application services that reside locally or on remote resources.
	3. Add the application services that you want to manage.
	  You can add application services in bulk with a CSV file. You can discover services on hosts with the `discover-services` utility, save the results to a CSV file, and upload the file.
	4. Select the credential that you want to use for running the application server.
	5. Apply the configuration, by selecting one of the following options:
	  • Apply configurations automatically. See "Setting up a scheduled task for reconfiguring services in Windows" on page 145.
	  • Apply configurations manually. See "Reconfiguring managed Windows services with changed credentials" on page 144.

Application fingerprints

The application registration 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 20. Properties that can be used for fingerprinting with different application types..

Property	Compiled Application	Scripts	Java EE Application	Application services
Host name	Yes	Yes	Yes	Yes
Operating System User	Yes	Yes	Yes	Yes
Group Name	Yes	Yes	Yes	No
Host Time Zone	Yes	Yes	Yes	Yes
Network Interfaces	Yes	Yes	Yes	Yes
Operating System	Yes	Yes	Yes	Yes
Architecture	Yes	Yes	Yes	Yes
Binary Path	Yes	No	No	No
Binary Hash	Yes	No	No	No

Host name
Fully 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 that is used to connect to the Privileged Identity Manager server is used for fingerprint matching.

Operating system
Name of the host operating system.

Binary path
The path to the JAR file containing the class that uses `AppIDManager`.

Binary hash
SHA 256 hash value of the class that calls the `AppIDManager # getCredential()` function.

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 change.

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 token. This option can be used for disaster recovery instances that are 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. For managed application services, the command line tool is used to register a service management agent. The command line tool is also used to reconfigure managed application services with changed credentials on endpoints that reside within the same Windows domain.

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 134. 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 136. 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:

   ```
   remote1
   ```

   ```
   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="remote1";
   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 134. 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.

   You must define the App ID data source in the **node** or **server** scope, instead of **cluster**.

   The fingerprint of each WebSphere Application Server is different, so you must register the data source in each node as separate app instances.

   Define the original data source in any scope as long as it is visible from the App ID data source's scope.

   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 21. 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" on page 134.

   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.

Rotating passwords for managed application services

You can rotate passwords of managed application services manually or automatically.

Before you begin

- Set up the service management agent.
- If you are managing application services on remote endpoints, prepare the endpoints.

Procedure

1. On-board the credentials and set up periodic password rotation, by using Service Center or a CSV file. See the following topics:
   - "Adding credentials in the Privileged Identity Manager Service Center" on page 51.
   - "Connecting a credential to an identity provider" on page 55.
   - "Specifying non-exclusive shared access credentials" on page 58.
   - "Configuring a reset interval for credentials" on page 57.
2. On-board the services to be managed, by using Service Center or by uploading a CSV file. See "Onboarding managed application services" on page 141.
3. Reset the password for a credential. See "Resetting credential passwords and SSH Keys" on page 55.
4. Apply the application service reconfiguration task. See "Reconfiguring managed Windows services with changed credentials" on page 144.

   When the credentials are reset, the service management agent completes the following tasks.
   a. Reconfigures the accounts for the service.
   b. Restarts the service, if configured.
   c. Sends an email notification, if configured.

   Note: To apply configurations automatically at specific periods, see "Setting up a scheduled task for reconfiguring services in Windows" on page 145.

Managed applications

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 ibmappid.jar
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 applications

Use the **Manage Applications** page in the Privileged Identity Manager Service Center to browse, search, and delete the applications and 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 fingerprints" on page 127.

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.

Managed application services

The tasks for managed application services include registering a service manager, preparing endpoints for remote application service reconfiguration, and onboarding application services.

With managed application services you can rotate passwords on both Windows services and scheduled tasks that are distributed across Windows hosts.

Credential changes for application services are administered by a service management agent. Application service reconfiguration on remote computers are performed remotely by the service management agent over WMI. If the computers belong to a Windows domain, the computers must belong to the same Windows domain.

If the credentials that you want to manage belong to a domain, you must install and configure a Windows Active Directory Adapter. For information, see "Identity provider management" on page 66.
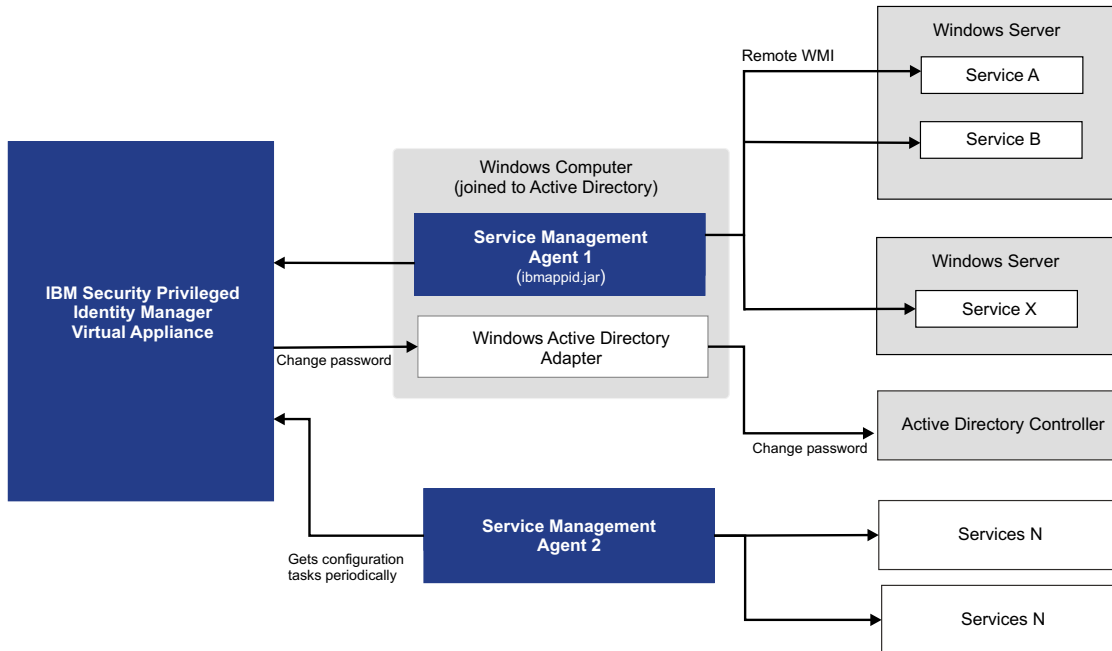
Figure 4. You can deploy service management agents on one or many computers. The agent can manage services local or remote computers. The example shows you how agents can manage application services on endpoints that belong to a Windows Active Directory domain.

If the credentials that you want to manage are local Windows accounts, ensure that the Windows Local Account Adapter is installed on each individual endpoint.

When services are reconfigured, email notifications are sent. The email notification for reconfigured services is defined by the **Application Service Reconfiguration Template** email template. For more information, see "Workflow notification properties" on page 189.

Registering a service management agent on a designated Windows host

You can use the service management host to manage application services that reside locally or on remote endpoints that belong to the same Windows domain.

Before you begin

- Enable and start the **Windows Management Instrumentation** service.

  Click **Start** > **All Programs** > **Administrative Tools** > **Services**.

- Configure the local computer firewall to allow traffic from the **Windows Management Instrumentation** service.

  Click **Start** > **All Programs** > **Administrative Tools** > **Windows Firewall with Advanced Security**.

- Get entitlements to a set of managed credentials. Entitlements let you verify that passwords for application services are reset correctly when you verify the configuration of services in the self-service interface. See "Access management" on page 70.

- Ensure that the Java runtime environment is installed.

  The Java runtime is used to run the command-line utilities in the App ID Toolkit.

About this task

You can use Service Center to administer managed application services with the service management host.

You register a workstation for managing application services by running the command line tool in the App ID Toolkit (`ibmappid.jar`) on the computer that you designate as the service management agent.

You can register more than one service management agent on the same workstation.

Procedure

1. Place the App ID Toolkit on the service management host.
2. Run the **register-service-manager** command:

   java -jar ibmappid.jar **register-service-manager** -s pimva.example.com
3. 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 ibmappid.jar
Enter server URL:	-s --server	URL of the IBM Security Privileged Identity Manager Server
Enter service management agent name:	-n --service-manager	Name of the service management agent.
Enter the operating system user who will run the service management agent:	-o --os-user	Operating system user name, the service manager will run under this user name, default: current user If you are registering a service management agent 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 service management agent" during registration must match the output of the whoami command for that user. For example, consider you are registering a service management agent 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.

For example:

```
C:\pim>java -jar ibmappid.jar register-service-manager —s ispim.example.com
Enter path of workspace folder (default: C:\pim):
Enter user name: valerie
Enter password:
Enter the OS user who will run the service management agent (default: valerie): EXAMPLE\AccountMgr
Enter service management agent name: services-on-42
```

The process completes successfully with this message: `(Service management agent name) created successfully`.

4. Optional: Set up a Windows scheduled task to automatically apply configurations to services with the **configure-services** command. See "Setting up a scheduled task for reconfiguring services in Windows" on page 145.

Preparing endpoints to allow remote service administration

Configure the endpoints to allow application services on the endpoint to be administered remotely by the service management workstation.

Before you begin

If you are managing credentials that are local Windows accounts on the endpoint, obtain the installation files for the Windows Local Account adapter.

About this task

By completing the necessary steps to grant access, the service management workstation can stop, restart, and update the configurations of application services on managed endpoints.

Procedure

1. Enable and start the **Windows Management Instrumentation** service. Click **Start** > **All Programs** > **Administrative Tools** > **Services**.

2. Configure the local computer firewall to allow inbound traffic from the **Windows Management Instrumentation** service.

   a. If the local Windows Firewall utility is enabled, click **Start** > **All Programs** > **Administrative Tools** > **Windows Firewall with Advanced Security**.

   b. In the navigation tree, click **Inbound Rules**.

   c. Ensure that the **Windows Management Instrumentation** rules are enabled.

3. Install the appropriate adapter, if needed.

   - If you are managing credentials that are local Windows accounts, where the Local Windows Account adapter is used, install the necessary Local Windows Account Adapter agent on each endpoint.

   - If you are managing credentials on endpoints that belong to a Windows Active Directory domain, you do not have to install the Active Directory Adapter on each endpoint.

4. If you are performing remote management of Windows services, prepare an Active Directory user that has WMI-related privileges: Execute Methods, Full Write, Enable Account, Remote Enable, Read Security, and Edit Security.

Onboarding managed application services

You can onboard managed Windows services and Windows Task Scheduler tasks by using service center or by loading managed instances from a CSV file.

Procedure

- Onboard Windows services by adding application services individually.
    1. Open Service Center.
    2. Click **Manage Applications**.
    3. Select an instance for application services. If the Windows service management agent is not yet set up, see "Registering a service management agent on a designated Windows host" on page 139.
    4. Click **Create**.
    5. Specify the following information for the service:

Table 22. Onboarding managed application services.

Type	Description

Windows service	**Name** Specifies a name for the service.
	
	Host Specifies the host where the service is running on.
	
	Service short name
	Specifies a short name for the service. The name must match the name of the Windows service.
	
	Service display name
	Specifies the displayed name associated with the service. This field is a descriptive name for the service.
	
	Notify email
	(Optional) Specifies the email addresses that receive email notifications. You can separate multiple email addresses with a comma (,).The domain administrator and the person with the email address specified are notified when there are email notifications.
	
	If there are no email addresses specified, the domain administrator and the system administrator are notified.
	
	Credential
	(Optional) Specifies the managed credential that you want to associate with the service.
	
	After configuration
	Specifies the action to take on the service after configuration.
	
	    Restart If the Windows service credential for a service is changed, and the service is currently running, the following actions take place:
	        1. The service is stopped.
	        2. The credential for the service is changed.
	        3. The service is started.
	
	        If the service is not running, the credential is changed, but the service is not started.
	
	    Do nothing
	        The credential for the service is changed. The state of the service is not changed.

Table 22. Onboarding managed application services. (continued)

Type	Description
Windows scheduled task	**Name** Specifies a name for the scheduled task.
	Host Specifies the host where the Windows task is running on.
	Target unique name Specifies a short name for the task. The name must match the name of the Windows scheduled task.
	Target display name Specifies the displayed name associated with the task. This field is a descriptive name for the task.
	Notify email (Optional) Specifies the email addresses that receive email notifications. If no email addresses are specified, the domain administrator is still notified. Separate multiple email addresses with a comma (,).
	Credential (Optional) Specifies the managed credential that you want to associate with the task.

- Onboard Windows services in bulk from a CSV file. See "Uploading a CSV file for application services with Service Center" on page 146.

  1. Prepare the CSV file.

     Note: You can use the `discover-services` command to discover available services on computers and save the results to a CSV file.

     To learn more about the CSV file format and columns, see "#ManagedInstances type identifier column headers" on page 107.

  2. Upload the CSV file.

Reconfiguring managed Windows services with changed credentials

Managed application services can be reconfigured with credentials that are managed by IBM Security Privileged Identity Manager. By using a managed credential, you can rotate passwords for a Windows service or a scheduled task.

Before you begin

Register a workstation as a service management agent.

About this task

Enforce periodic password rotation on all non-default Windows services across a set of Windows hosts to comply with corporate security policies. You can also enforce periodic password rotation on Windows scheduled tasks that run by using a credential. Automatic password rotation with the service management agent avoids the need for the Windows service administrator to manually update various Windows services.

Procedure

On the service management agent workstation, run the **configure-services** command line tool.
For example:
```
java -jar ibmappid.jar configure-services -n service_manager_name -s
ispim.example.com -w c:\appid
```

Setting up a scheduled task for reconfiguring services in Windows

To configure services periodically with the service management agent, set up a scheduled Windows task by using the Windows Task Scheduler.

Procedure

1. Click **Start** > **All Programs** > **Administrative Tools** > **Task Scheduler**.
2. Right-click Task Scheduler Library, and select **Create Task**.
3. In the General tab, specify a name for the task.
4. Under **Security options**, select **Run whether user is logged on or not**.
5. Under the **Trigger** tab, click **New**.
6. Specify how often you want to run the task. For example, you can run the task every day in the evening from 7pm.
7. Under the **Actions** tab, click **New**.
8. For **Action**, select **Start a program**.
9. Specify the following options:

Field	Value
Program/Script	`java`
Add arguments (optional)	`-jar ibmappid.jar` **configure-services** `-n` *services-on-42* `-s` *pimva.example.com* `-w` `C:\appid -x`
Start in (optional)	`C:\appid`

10. If required, enter the user account information that is running the task.
11. Click **OK**.

Suspending updates to application services

You can suspend the service management agent or individual services so that updates selected application services are disabled. You can choose to resume updates to application services again at a later time.

Procedure

1. In Service Center, click **Manage Applications**.
2. To suspend updates to application services, do one of the following tasks:
   - To suspend all the updates that are managed by a registered service management agent:
     a. In the left application pane, select a registered service manager.

     b. Click **Suspend Service Manager** ⏸ .

        A suspended service manager will have a SUSPENDED indicator below its description.

- To suspend updates to a specific application service, in the Managed Application Services area, click **Active** cell.

3. To resume the process of applying configuration updates to application services, do the following tasks:
   - To restore configuration updates for a service management agent that has been suspended, select the agent, and click **Restore** ⊙ .
   - To restore configuration updates to individual services that have been deactivated, click **Active**.

Uploading a CSV file for application services with Service Center

As a Privileged Administrator, you can add or update the list of managed application services that are specified in a comma-separated value (CSV) file with the Service Center.

About this task

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

If there are related credentials defined in the CSV file, the credentials must use the `#Credentials_v2` type identifier. See "#Credentials_v2 type identifier column headers" on page 99.

Important: The **ACCESS_MODE** must be set to 1.

Restriction: The maximum number of entries in the CSV file is 1,000.

Procedure

1. From Service Center, click **Manage Applications**.
2. In the left pane, select a service management agent.
3. In the **Managed Application Services** area, click **Update**. The Upload CSV File page is displayed.
4. Optional: In the **Upload Name** field, type a name to identify the upload operation.
5. Click **Browse** to locate the CSV file.

   Note: The file must have the CSV file type extension, `.csv`.
6. Submit the request. 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 application services that are defined in the CSV file to be managed by the service management agent.

What to do next

You can view the status of your request by selecting **View Requests** in the Administrative console. The tasks in **View Requests** provides detailed information about the request.

Chapter 9. Services administration

A service is an identity feed that can be used for provisioning IBM Security Privileged Identity Manager users.

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

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.

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.

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**.

Identity Feed types

The default identity feed 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.

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 154.

- To change a service, see "Changing identity-feed services" on page 157.
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 Privileged Access Agent for automatic checkout. Privileged Access Agent 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 246
- "Specifying owners of a role" on page 251

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 154
Create an instance of a service from a service type, such as the DSML service.

"Changing identity-feed services" on page 157
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 Privileged Access Agent 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. Log in to the administration console and select **Configure System > Design Forms**.
2. Perform one of the following actions:
   - Open a file with the Java Web Start Launcher and click **OK**.
   - Save the file and run it with the Java Web Start Launcher at a later time.
3. In the left pane of the Design Form window, double-click the **Service** folder.
4. Double-click a profile to open the form template. For example: **POSIX Linux Profile**.

Note: You see the **$servicetabgeneral** tab by default.

5. From the **Attribute List** box, select the **eruri** attribute and click the **Add Row** icon to add it to the form.

6. Select the $eruri attribute and then click the **Editable Text List** icon. The $eruri attribute is a multivalue attribute.

7. With the $eruri selected, type a new label name in the **Label** field in the **Format** tab in the **Properties** box. 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 click **OK**.

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 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.

Reconciliation for identity-feed services

Initiate a reconciliation activity on identity-feed service

Before you begin

You must complete the steps for configuring a identity service type to support groups. You must also have created a identity feed 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.

Chapter 10. Group administration

IBM Security Privileged Identity Manager provides predefined groups. As a System Administrator, 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 aIBM Security Privileged Identity Manager user can perform.

Before you begin

If a new group requires a new business unit, create the business unit first.

About this task

You can use the Create Group wizard to create more groups.

Procedure

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.

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.

Adding members to groups

You can add members to groups.

Procedure

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. 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 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 a System 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

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

As a System Administrator, you can delete groups from the Administrative console.

About this task

You cannot delete a group that has members.

Procedure

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 11. 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**.

Session policies

Specify settings for sessions that are launched with the Privileged Session Gateway.

Configuring session policies

A System Administrator can specify the settings for sessions that are launched with Privileged Session Gateway.

Procedure

1. Log in to the Administrative console.
2. Select **Configure Sessions** > **Configure Session Policies**.
3. On the **Configure Session Policies** page, the following policies are set by default:
   - **Check in the credential by default** is not selected.
   - **Allow the user to specify if the credential should be checked in** is selected.

   Note:
   - If the **Check in the credential by default** policy is not selected, the credential is not returned when the session is ended.
   - If the **Allow the user to specify if the credential should be checked in** policy is selected, the user is given an option to return the credential when a session is ended.
   - The default setting does not return the credential when the session ends. It gives users an option to check in a credential when the session is ended or at a later time in the Self-service console.
4. In **Resource Tags**, specify one or more resource tags. Credentials that are associated with the resource, with the specified tags are allowed to initiate a session from the Self-service console.

   Note:
   - By default, there are no resource tags specified and the Privileged User can initiate a session.
   - The Privileged User cannot initiate a session with the credential, if the resource associated with the credential does not contain the specified tags.
5. Click **Submit**.

Configuring a session recording policy

As a System Administrator, you can configure recording policies from the Administrative console for sessions that are launched with Privileged Session Gateway.

Procedure

1. Log in to Administrative console.
2. Select **Configure Sessions** > **Configure Session Recording Policies**.
3. On the **Configure Session Recording Policies** page, select the check box to record sessions that are launched with Privileged Session Gateway.

   Note: If the check box is not selected, sessions are not recorded.
4. Click **Submit**.

Privileged Access Agent policies

As a System Administrator, you can configure the credential prompt and recording options for application logons with Privileged Access Agent in AccessAdmin.

Use the AccessAdmin privileged identity management policies to configure application logon sessions with Privileged Access Agent.

pid_recorder_enabled: Enable session recording?

IMS Entry	Enable session recording?
Location	**AccessAdmin** > **System** > **System policies** > **IBM Security Privileged Identity Manager Configuration Policies**
Description	Whether to record sessions created using shared access identities.
Registry	
Type	Boolean
Values	• No • Yes (default, if session recording feature is activated)
Scope	System
Note	Refreshed on sync.

pid_recorder_image_capture_option: Session recording image capture option

IMS Entry	Session recording image capture option
Location	**AccessAdmin** > **System** > **System policies** > **IBM Security Privileged Identity Manager Configuration Policies**
Description	Color depth of the images to capture for session recording.
Registry	
Type	Non-negative integer
Values	• #0: Full Color • #1: Grayscale (default value)
Scope	System
Note	Refreshed on sync.

pid_recorder_keyboard_capture_option: Session recording keyboard capture option

IMS Entry	Session recording keyboard capture option
Location	**AccessAdmin** > **System** > **System policies** > **IBM Security Privileged Identity Manager Configuration Policies**
Description	Specifies keyboard events to capture during a screen-based session recording.
Registry	
Type	Non-negative integer
Values	• #0: Log all key inputs (default value) • #1: Log only special keys • #2: Do not log any key inputs
Scope	System
Note	Refreshed on sync. This option does not apply to text-based recordings.

pid_collector_comm_fail_action: Action to take when the client computer cannot connect to the server

IMS Entry	Action to take when the client computer cannot connect to the server
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Specifies the action to take on the client computer when the Privileged Session Recorder Server is not reachable after a maximum number of retries.
Registry	
Type	Non-negative integer
Values	• #0: Take no action. (default) • #1: Block user inputs. • #2: Close application.
Scope	System
Note	Refreshed on sync.

pid_collector_comm_fail_limit: Maximum number of failed connection attempts to the server

IMS Entry	Maximum number of failed connection attempts to the server
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Specifies the maximum number of connection attempts before determining that the Privileged Session Recorder Server is not reachable.
Registry	
Type	Non-negative integer
Values	3 (default value)
Scope	System
Note	Refreshed on sync.

pid_collector_comm_fail_retry_interval: Time interval between connection retries to the server

IMS Entry	Time interval between connection retries to the server
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Time interval, in seconds, between attempts to connect to the Privileged Session Recorder Server.
Registry	
Type	Non-negative integer
Values	15 (default value)
Scope	System
Note	Refreshed on sync.

pid_pim_optional_justification

IMS Entry	Allows empty justification on credential check out.
Location	**AccessAdmin > System > System policies > IBM Security Privileged Identity Manager Configuration Policies**
Description	Allows privileged users to check out credentials without entering a justification.
Type	Boolean
Values	• Yes • No (default)
Scope	System
Note	Refreshed on sync.

Applying a user policy template

After you create a User Policy Template, you must apply it to your users so that the policies are implemented.

Procedure

1. Log on to AccessAdmin.
2. Select **Search users** > **Search**.
3. Enter the subject of your search in the **Search for** field.

   Tip: To find partially matching results, enter the characters, and then an asterisk (*). For example: To find all users with user names that begin with the letter i, enter i*.

   a. Select a search criteria from the **Search by** list.

   b. Click **Search**.
4. Optional: Select any of the following groups:
   - My users
   - All Administrators
   - All help desk users
   - All revoked users
5. Specify the number of results to view per page.
6. Select one or more users by selecting the check box next to the corresponding user. Click **Select all** if you want to assign policies to all users in the page.
7. Select the template that you want to apply under **Apply user policy template**.
8. Click **Apply to selected results**. **Apply to all results** is applicable to the users displayed on the page.

Chapter 12. 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 access request workflow

As a System Administrator, you can create 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 a simple workflow.
   a. Click to **Add** a workflow that consists of a linear series of approval, mail, or request for information activities.
   b. To **Create an approval activity**, complete the activity name, participant type, and escalation time and escalation participant type. Then, click **OK**.
   c. To **Create a mail activity**, complete the activity name, participant type, and mail content. Then click **OK**.
5. On the Success page, click **Close**.

What to do next

You can associate this workflow with an access that is assigned by request.

Changing an access request workflow

As a System Administrator, you can 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 access request workflow

As a System 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 any access.

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	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**.
Advanced	1. After the workflow designer applet starts, select the Mail node. Then, copy (click and drag) an instance of the Mail node to the Workflow Diagram workspace. Double-click the Mail node instance to open the Properties: Mail Node page. a. In the General tab, make these entries: • In the **Activity ID** field, type a value that identifies the activity, such as `mytesttemplate`. • In the **Recipient** field, select a recipient from the list. • Optionally, type a value for the activity name, and change the default value of the Join Type and Split Type conditions. b. In the Notification tab, either type the tags and other information that you want to be displayed in a customized message notification, by completing the **Subject**, **Text**, and **XHTML** fields as needed. Alternatively, click **Load From Template**. If you load a template, complete these tasks: • In the templates table, select a template. Then, click a button such as **Create Like**. • On the Mail Activity Template page, accept or modify the entries that populate the **Template Name**, **Subject**, **Text**, and **XHTML** fields. • Change the Text and Dynamic entries as needed. Then, click **OK**. c. In the Postscript tab, type any postscript information. d. Click **OK** to complete the task. Depending on the customized steps that you took or the template that you selected, you might need to change the notification recipient.

5. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
6. On the Success page, click **Close**.

Creating Web Service Integrations

As a System Administrator, you can create Web Service Integrations.

Before you begin

Import signer certificate of the web service, if required. See Managing certificates.

About this task

Web Service Integrations provide a way for IBM Security Privileged Identity Manager to integrate with other applications through web service calls.

You can use the **Manage Web Service Integrations** page in the Administrative console to create a web service integration template that specifies content to be used by activities across different operations.

Note: To substitute parts of the value with variables from an operation, click on **Macro list** for a list of macros for the Web Service Call definition. See "Macro List" on page 182

Procedure

1. In the Administrative console, click **Configure System** > **Manage Web Service Integrations**.
2. Click **Create**.
3. Provide the information in the following table:

Tab	Procedure	
General	**Name**	Specify a name for the Web Service Integration. It is used in the extension node, under **Extension Name** when you are defining an operation. See "Define an operation with the Web Service Integration" on page 184.
		Note:
		• The Web Service Integration name can only contain letters and numbers. It cannot contain spaces.
		• When you are cloning an existing Web Service Integration, specify a different name for the cloned Web Service Integration. Two Web Service Integrations cannot share the same name.
	Description	
		Specify a description for the Web Service call.
	Request URL	
		Specify the URL for the Web Service call.
	HTTP verb	
		Specify a HTTP verb from the drop-down list.
Authorization	**Type**	Specify one of the following authorization types from the drop-down list:
		• **Basic Authentication**- A user name and password is required to make a request.
		• **Access Token (OAuth 2.0)**- An access token to make API requests on behalf of the user. **Note:** You need to perform the authorization grant before you set up the Web Service Integration. IBM Security Privileged Identity Manager does not support performing OAuth 2.0 authorization flows.
		Note: Specify **None** from the drop-down list if you want to customize an authorization. You can customize the authorization in the **Headers** tab.

Tab	Procedure
Headers	**Name** Specify a name for the request header. **Value** Specify a value for the request header. You can also specify multiple values (comma-separated. For example: 1,2,3. **Note:** Do **not** specify the same header more than once, as the values are modified.
URL Query Parameters	**Name** Specify a name for the query parameter. **Value** Specify a value for the query parameter.
Body	**Encoding (Content-Type)** Specify an encoding type from the drop-down list: • The **Raw** and **JSON (application/json)** encoding types require you to type the entire request body. • The **form-data** and **x-www-form-urlencoded** encoding types requires you to specify name-value pairs, which are used to construct a request body of the expected type.

Response Output	**Response Parser**
	 Specify a response parser from the drop-down list. Depending on the response parser that you select, you are required to provide more information. You can specify multiple parsers. See the following response parsers:
	
	 • The **Expect status code**, **Expect header value**, and **Expect body regular expression** parsers expect a certain value. The activity is marked rejected if the value is not returned by the web service.
	
	 • The **Return status code**, **Return header**, and **Return body** parsers return a value as an output parameter for the operation.
	
	 • The **Return Body Regular Expression group** parser returns the string from the body that matches the first parentheses group in the regular expression. If there is no group specified, the string matching the entire regular expression is returned.
	
	 • The response body must be in XML for the **Return Body XPath** parser. The value matching the XPath is returned.
	
	 • The response body must be JSON for the **Return Body JSONPath** parser.
	
	 The format of the path elements:
	
	 dot notation
	 jsonObject.name- name cannot contain dot or left bracket. A backslash can be used to quote characters.
	
	 Bracket notation
	 jsonArray[number] number must be an integer.
	
	 jsonObject['name'] name cannot contain quote. A backslash can be used to quote the quote.
	
	 jsonObject["name"] name cannot contain double quote. A backslash can be used to quote the double quote.
	
	 The path evaluation starts at the root of the JSON object.
	
	 The path can start with bracket notation.
	
	 For example, if the body is
	
	 `{ "name:`
	 `{ "first" : "John",`
	 `"last" : "Smith"`
	 `}`
	 `}`
	
	 With a path of name.last. The return value is Smith.
	
	 If the body is
	
	 `[ { "addr": {"City": "London},`
	 `"name": { "first" : "Joan", "last" : "Smith" } } ]`
	
	 With a path of [0].name.first, the return value is Joan.

4. Click **OK** to save the template.

What to do next

To configure an operation to call the web service integration, see "Define an operation with the Web Service Integration" on page 184.

Macro List

This page lists the macros that are substituted when you are performing a web service call.

Macros	Description
$CREDENTIAL.NAME	Specifies the name of the credential.
$CREDENTIAL.DESCRIPTION	Specifies the description for the credential.
$RESOURCE.NAME	Specifies the resource name.
$RESOURCE.UID	Specifies the resource unique ID.
$PERSON.USERID	Specifies the user ID of the person who is performing the operation.
$PERSON.NAME	Specifies the full name of the person who is performing the operation.
$PERSON.MAIL	Specifies the email address for the person who is performing the operation.
$PERSON.PHONE	Specifies the telephone number for the person who is performing the operation.
$PERSON.MOBILE	Specifies the mobile telephone number for the person who is performing the operation.
$PERSON.HOMEPHONE	Specifies the home telephone number for the person who is performing the operation.
$PERSON.PAGER	Specifies the pager number for the person who is performing the operation.
$DOMAINADMIN.USERID	Specifies the user ID for the domain administrator.
$DOMAINADMIN.MAIL	Specifies the email address for the domain administrator.
$DOMAINADMIN.PHONE	Specifies the telephone number for the domain administrator.
$DOMAINADMIN.MOBILE	Specifies the mobile telephone number for the domain administrator.
$DOMAINADMIN.HOMEPHONE	Specifies the home telephone number for the domain administrator.
$DOMAINADMIN.PAGER	Specifies pager number for the domain administrator.
$LEASE.CUSTOM1	Specifies the custom attribute 1 for the lease.
$LEASE.CUSTOM2	Specifies the custom attribute 2 for the lease.
$LEASE.CUSTOM 5	Specifies the custom attribute 5 for the lease.
$LEASE.JUSTIFICATION	Specifies the justification for the lease.

Macros	Description
$RELEVANTDATA.*id*	An item from the Relevant data that is specified by *id* in the operation properties. **Note:** This ID is **not** the ID that is specified in the Web Service Integration form in the response output.

Modifying Web Service Integrations

As a System Administrator, you can modify existing Web Service Integrations.

About this task

When there is an operation that is using an existing Web Service Integration, modifying the name of the Web Service Integration affects the operation. You are required to manually update the extension node that is defined in the operation where the Web Service Integration is used with the new Web Service Integration name.

Similarly for return output parameters, if there are any modifications to the return output parameters of a Web Service Integration, the System Administrator must manually refresh the extension node in the operation that uses the modified Web Service Integration as the selected activity. For example, adding a new return output parameter or deleting any existing return output parameters.

Important: Follow the procedure below to refresh the extension node in **Manage Operations**:

1. In the **Operation Diagram**, open the extension node that uses the modified Web Service Integration.
2. On the **Extension Name** drop-down field, select any other activity type, and then re-select the activity type for the modified Web Service Integration. The updated Output Parameters is displayed. The System Administrator must map the updated output parameters to the intended Relevant Data IDs.
3. Click **OK** and **Save** the operation.

You can modify an existing header by adding a header with the same name, with new or additional values. Adding a new header with a header name that already exists does not create a new header. For example, if there is an existing `test-header` with value 1, adding another `test-header` with value 2, modifies the header value from 1 to 2. You cannot specify headers of similar name with different values. If you are modifying values (comma-separated), you must type the full string, including the value that was previously provided. For example, if `test-header` has value 1 and you want to add values 2 and 3, you must type values `1,2,3` to modify the header. The modified header and its values are automatically refreshed in the extension node that is defined in the operation where the Web Service Integration is used.

Procedure

1. In the Administrative console, click **Configure System** > **Manage Web Service Integrations**.
2. Click **Change**.

Deleting Web Service Integrations

As a System Administrator, you can delete Web Service Integrations that are no longer needed.

Procedure

1. In the Administrative console, click **Configure System** > **Manage Web Service Integrations**.
2. Select the Web Service Integration to delete and click **Delete**.

   Note: You cannot delete a Web Service Integration that is being used in an operation. Deleting it results in an operation error when the operation is run.

Define an operation with the Web Service Integration

As a System Administrator, you can customize different operations with the Web Service Integration to fit your requirements.

About this task

The Web Service Integration that you create is used in the extension node, under **Extension Name** when you are defining an operation.

The following macros are available when you are performing a check-out operation:

Macros	Description
$CREDENTIAL.NAME	Specifies the name of the credential.
$CREDENTIAL.DESCRIPTION	Specifies the description for the credential.
$RESOURCE.NAME	Specifies the resource name.
$RESOURCE.UID	Specifies the resource unique ID.
$PERSON.USERID	Specifies the user ID of the person who is performing the operation.
$PERSON.NAME	Specifies the full name of the person who is performing the operation.
$PERSON.MAIL	Specifies the email address for the person who is performing the operation.
$PERSON.PHONE	Specifies the telephone number for the person who is performing the operation.
$PERSON.MOBILE	Specifies the mobile telephone number for the person who is performing the operation.
$PERSON.HOMEPHONE	Specifies the home telephone number for the person who is performing the operation.
$PERSON.PAGER	Specifies the pager number for the person who is performing the operation.
$DOMAINADMIN.USERID	Specifies the user ID for the domain administrator.
$DOMAINADMIN.MAIL	Specifies the email address for the domain administrator.
$DOMAINADMIN.PHONE	Specifies the telephone number for the domain administrator.

Macros	Description
$DOMAINADMIN.MOBILE	Specifies the mobile telephone number for the domain administrator.
$DOMAINADMIN.HOMEPHONE	Specifies the home telephone number for the domain administrator.
$DOMAINADMIN.PAGER	Specifies pager number for the domain administrator.
$LEASE.CUSTOM1	Specifies the custom attribute 1 for the lease.
$LEASE.CUSTOM2	Specifies the custom attribute 2 for the lease.
$LEASE.CUSTOM 5	Specifies the custom attribute 5 for the lease.
Macros	Description
$CREDENTIAL.NAME	Specifies the name of the credential.
$CREDENTIAL.DESCRIPTION	Specifies the description for the credential.
$CREDENTIAL.TAG	Specifies the credential tags for the credential. If there are multiple values, credential tags are comma separated.
$RESOURCE.NAME	Specifies the resource name.
$RESOURCE.UID	Specifies the resource unique ID.
$RESOURCE.TAG	Specifies the resources tags for the resource. If there are multiple values, resource tags are comma separated.
$RESOURCE.ALIAS	Specifies the resource alias for the resource. If there are multiple values, resource aliases are comma separated.
$IDP.NAME	Specifies the identity provider name.
$IDP.TYPE	Specifies the identity provider type.
$PERSON.USERID	Specifies the user ID of the person who is performing the operation.
$PERSON.NAME	Specifies the full name of the person who is performing the operation.
$PERSON.MAIL	Specifies the email address for the person who is performing the operation.
$PERSON.PHONE	Specifies the telephone number for the person who is performing the operation.
$PERSON.MOBILE	Specifies the mobile telephone number for the person who is performing the operation.
$PERSON.HOMEPHONE	Specifies the home telephone number for the person who is performing the operation.
$PERSON.PAGER	Specifies the pager number for the person who is performing the operation.
$DOMAIN.NAME	Specifies the name of the domain.
$DOMAINADMIN.USERID	Specifies the user ID for the domain administrator.
$DOMAINADMIN.MAIL	Specifies the email address for the domain administrator.
$DOMAINADMIN.PHONE	Specifies the telephone number for the domain administrator.

Macros	Description
$DOMAINADMIN.MOBILE	Specifies the mobile telephone number for the domain administrator.
$DOMAINADMIN.HOMEPHONE	Specifies the home telephone number for the domain administrator.
$DOMAINADMIN.PAGER	Specifies pager number for the domain administrator.
$LEASE.CUSTOM1	Specifies the custom attribute 1 for the lease.
$LEASE.CUSTOM2	Specifies the custom attribute 2 for the lease.
$LEASE.CUSTOM5	Specifies the custom attribute 5 for the lease.
$LEASE.JUSTIFICATION	Specifies the justification for the lease.
$LEASE.EXPIRATIONTIME	Specifies the lease expiration date and time in ISO 8601 format.

These macros, if used, are populated during a check-out process. If you specified a response output in the Web Service Integration, you can specify a relevant data for the output parameter when you are defining the operation. Once specified, you can use the relevant data in other extension nodes that are within the same operation or you can use the $RELEVANTDATA.*id* macro when you are creating other Web Service Integrations.

Follow the procedure below to specify the $RELEVANTDATA.*id* macro in **Manage Operations**:

1. In the **Operation Diagram**, click **Properties**.
2. In the **Relevant Data** section, click **Add** to specify an ID and type.
3. In a **Script** node, specify the values in the Javascript field.

You can also store cookies received from a Web Service call. All calls within the same operation that use the same cookie jar automatically include cookies that are stored in that jar. You can reuse the cookies in the next Web Service Integration that requires existing cookies.

Follow the procedure below to specify a cookie jar:

1. In the **Operation Diagram**, click **Properties**.
2. In the **Relevant Data** section, click **Add**.
3. In the **ID** field, specify **Cookies** and in the **Type** list, select **Map**.

Scenario: Integrating with an Incident Management System with the Web Service Integration to check out credentials for incident validation

In this scenario, an incident management system provides an API to retrieve information for specific incidents that require the following requests:

- Verifying that an incident ID has been assigned to the current user. For example, GET/api/incidents/{id} returns:

  {"id": "12345", "summary": "verify incident id", "owner": "james"}

- Acknowledging an incident. For example, PUT/api/incidents/{id} returns:

  {"status": "acknowledged"}

- The requests are authenticated with an access token

If the Web Service Integration is configured correctly, when the privileged user receives a notification from the incident management system on an incident, he is able validate the incident ID and check out a credential to use.

In this scenario, as a System Administrator, perform the following tasks:

- Create two Web Service Integrations:

  1. **Check Incident ID**

     ```
     Name: checkIncidentID
     Request URL: https://example.com/api/incidents/$LEASE.CUSTOM1
     HTTP Verb: GET
     Authentication Type: Access Token
         Value (?): Bearer 147a840c1785564d...
     Response Output: Expect body regular expression
         \"owner"\"\*:\s*\"$PERSON.USERID\"
     ```

  2. **Acknowledge Incident**

     ```
     Name: acknowledgeIncident
     Request URL: https://exmaple.com/api/incidents/$LEASE.CUSTOM1
     HTTP Verb: PUT
     Authentication Type: Access Token
         Value (?): 123a654b89568c...
     Body: Encoding: JSON
         Value: {"status": "ACKNOWLEDGED"}
     Response Output: Expect Status Code 200
     ```

- Create a custom check-out operation. See "Define a checkout operation with the checkout extension" on page 199.
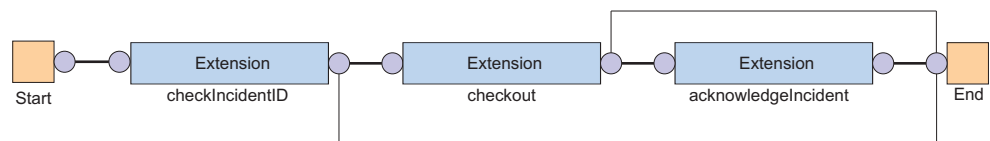
Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Extension	Activity ID	web_service_int_call
	Extension Name	Web Service Integration defined in "Creating Web Service Integrations" on page 180

Node	Feature	Value
Extension	Activity ID	checkout_operation
	Extension Name	checkout(Credential credential, CredentialLease leaseIn, Account account, Person person)
	Input Parameters	• credential - credential • leasein - credentialLease • account -account • person - lessee
	Output Parameters	leaseout - CredentialLease
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A

- Configure credential default settings to specify the **Check Out Operation Name**. See "Configuring the credential default settings" on page 111.
- Customize the check-out form to create a field to input the incident ID when checking out a credential. See "Customizing the checkout form" on page 113.

Creating an access request workflow

A privileged administrator can select the workflow to be used for each access.

About this task

The IBM Security Privileged Identity Manager administrator can create workflows that are started when a user requests access. Access request workflows are activities that are typically performed when users request access. Typically, this consists of approval and email notification.

After this workflow is created, a privileged user can request access to the managed resource.

For instance, if Judith User wants to access a managed resource, Judith can request access. The manager (Chuck Manager) is notified of the request. Chuck can approve or reject the request. If Chuck does not respond to the request within the specified period, the access owner must respond.

Procedure

1. Log in to the administrative console as PIM Manager.
2. From the navigation tree, select **Configure System** > **Manage Access Request Workflows**.
3. On the Manage Access Request Workflows page, in the **Access Request Workflows** table, click **Create**.
4. On the General notebook page, type the following information for your workflow:

   Name A name to identify the workflow. For example: Windows DBA server access workflow.

Description

A description of the intended purpose of the workflow. For example:
`Approval for the DBA group`.

Business unit

Indicates the business unit. Click Search to locate and select a business unit. This field is read-only when you are making a change to a workflow.

5. Click the **Activities** tab. On the Activities page, select **Create an approval activity** and click **Go**.

6. On the Approval Activity page, specify the following information and click **OK**:

Activity name

A name to identify the activity. For example: `Manager Approval for Windows DBA server access`.

Approver type

Users who can approve the request. For example: **Manager**.

Escalation time in days

The request escalates to the specified escalation participant when this interval of time expires. For example: `10`

Escalation participant type

Users who can approve the request after it has been escalated. For example **Access owner**.

7. On the Activities notebook page, click **OK** again.

8. 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
- Application service reconfigured

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

System Administrators can set the default escalation limit for work items in workflows.

Before you begin

Determine the escalation period that your organization needs

About this task

You can use the Workflow Notification Properties page to change the workflow escalation.

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"><PARM>
<JS> if (process.canceledDate != null) return process.canceledDate.getTime(); else return '';</JS></PARM></RE>
<JS> if (process.canceledBy != null) { '<RE key="CanceledReason"/>:
<JS> (process.canceledJustification == null)? '': process.canceledJustification;</JS>'; }</JS>
```

4. In the Notification Template page, modify the **XHTML body** field by adding this code inside the table:

```
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="CanceledBy"/>:</td><td width="773" class="text-description" bgcolor="white">
  <JS>process.canceledBy;</JS></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="DateCanceled"/>:</td><td width="773" class="text-description" bgcolor="white">
  <RE key="readOnlyDateFormat"><PARM>
  <JS>if (process.canceledDate != null) return process.canceledDate.getTime();
  else return '';</JS>
  </PARM></RE></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="CanceledReason"/>:</td><td width="773" class="text-description" bgcolor="white">
  <JS>process.canceledJustification;</JS></td></tr>
```

Place the new code inside the table between these two sets of existing code:

```
<pre><JS>Enrole.localize(process.resultDetail, "$LOCALE");</JS></pre></td></tr>
```

and

```
        </table>
            </td>
                    <!-- End Of Notification body -->
```

5. To save the changes, click **OK**.
6. On the Workflow Notification Properties page, click **OK**.
7. On the Success page, click **Close**.

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.
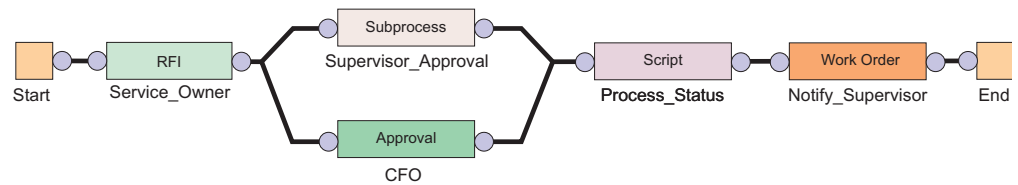
Figure 5. Sample workflow: multiple approvals required

Table 23. Node properties: Sample workflow for multiple approvals

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

Table 23. Node properties: Sample workflow for multiple approvals (continued)

Node	Feature	Value
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
Script	Activity ID	Process_Status
	Join Type	AND
	Split Type	AND

	JavaScript	`supervisorApproval=`
		`process.getActivity("Supervisor_Approval").result`
		`Summary`
		`cfoApproval=process.getActivity("CFO").resultSummary`
		`if(supervisorApproval==activity.APPROVED &&`
		`cfoApproval==activity.APPROVED)`
		`{ process.setResult(process.APPROVED) }`
		`else`
		`{ process.setResult(process.REJECTED) }`

Work Order	Activity ID	Notify_Supervisor
	Participant	Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Subject	New <JS>process.subject;</JS> provisioning request for <JS>process.requesteeName;</JS>
	Message	Process Result: <JS>process.resultSummary</JS>

Table 23. Node properties: Sample workflow for multiple approvals (continued)

Node	Feature	Value
End	Activity ID	End
	Join Type	AND
	JavaScript	N/A
Transition Line`Start > Service_Owner RFI`	JavaScript	[Custom] `true`
Transition Line`Service_Owner RFI > Supervisor_Approval Subprocess`	JavaScript	[Custom] `true`
Transition Line`Service_Owner RFI > CFO Approval`	JavaScript	[Custom] `true`
Transition Line`Supervisor_Approval Subprocess > Process_Status Script`	JavaScript	[Custom] `true`
Transition Line`CFO Approval > Process_Status Script`	JavaScript	[Custom] `true`
Transition Line`Process_Status Script > Notify_Supervisor Work Order`		[Custom] `true`
Transition Line`Notify_Supervisor Work Order > End`	JavaScript	[Custom] `true`

Sample workflow: RFI and subprocess

This example displays an entitlement workflow that uses an RFI and a subprocess.

For the request to be approved and reach completion, the following actions must occur:

- The workflow initiated by the Subprocess node must be completed with a result of approved.
- The participant defined in the RFI node is sent a request for information.

An approved response must come from the subprocess for the request to continue to the RFI.
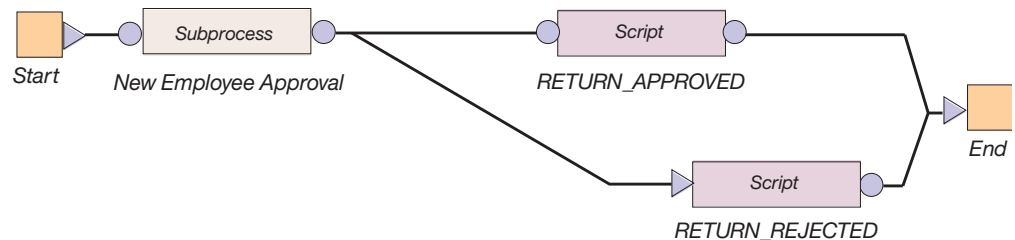
Figure 6. Sample workflow: RFI and subprocess

Table 24. 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
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	OR
	Split Type	OR
	JavaScript	`process.setResult` `(process.APPROVED);`
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	OR
	Split Type	OR
	JavaScript	`process.setResult` `(process.REJECTED);`
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A
Transition Line`Start > New Employee Approval`	JavaScript	[Custom] `true`

Transition Line`New Employee Approval > Request Storage Quota`	JavaScript	[Approved]
		`activity.resultSummary`
		`==activity.APPROVED;`

Transition Line`New Employee Approval > RETURN_REJECTED`	JavaScript	[Rejected]
		`activity.resultSummary`
		`==activity.REJECTED;`

Transition Line`Request Storage Quota > RETURN_APPROVED`		[Custom] `true`
Transition Line`RETURN_APPROVED > End`	JavaScript	[Custom] `true`
Transition Line`RETURN_REJECTED > End`	JavaScript	[Custom] `true`

Sample workflow: approval loop

This example displays a workflow that loops an Approval node.

In this workflow, the manager approval is set within the Loop node. The manager approval repeats five times before failing if an approved or rejected response is not received within the escalation Limit.

Conditions for the transition lines to the RETURN_APPROVED and RETURN_REJECTED script nodes must be defined to retrieve and evaluate the results of the Approval node. The loop node does not return a response from the Approval.
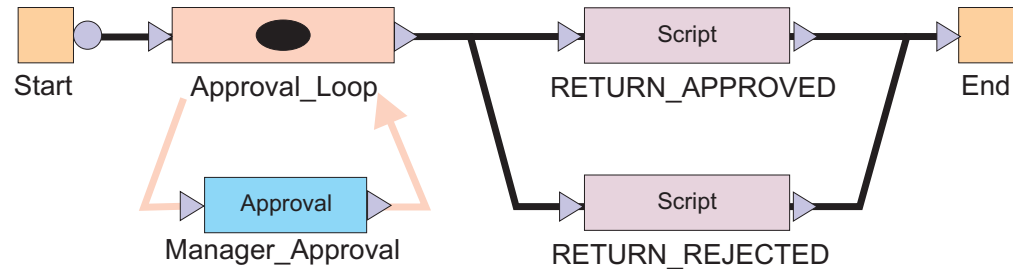
Figure 7. Sample workflow: approval loop

Table 25. 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);`

Node	Feature	Value
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A
Transition Line Start > Approval Loop	JavaScript	[Custom] `true`
Transition Line Approval Loop > RETURN_APPROVED	JavaScript	[Custom] `approvalFlag.get() == "APPROVED"`
Transition Line Approval Loop > RETURN_REJECTED	JavaScript	[Custom] `approvalFlag.get() == "REJECTED"`
Transition LineRETURN_APPROVED > END	JavaScript	[Custom] `true`
Transition LineRETURN_REJECTED > END	JavaScript	[Custom] `true`
Relevant DataapprovalFlag	ID	approvalFlag
	Description	Data for storing the last approval result
	Context	N/A
	Type	String
	Default Value	FALSE

Sample workflow: mail activity

Use the Workflow Designer page to create a mail activity workflow template that specifies content to be used by mail activities across different workflows.

Use this page to specify the contents and recipient of an email message. You can also create, change, or delete email templates used for defining contents of mail activities. To create a notification that uses an existing notification template as its initial content, or to create an entirely new notification, complete these steps:

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that appears, in the table that lists the workflows, click **Create**.
3. In the **General** tab, complete the name and description of the workflow, and select a business unit and service type.
4. In the **Activities** tab, click **Simple**.
5. In the **Simple Activities Definition** table, select **Create a mail activity**. Then, click **GO**.
6. In the Mail Activity page, complete the following fields:

   Activity name
   > Provides a name for the mail activity.

   Recipient type
   > Select a recipient for mail from the list. You might select **User name** or **Group**. An additional field is displayed for you to search for and specify a specific user or group that is not in the list.

   Load from Template
   > Click to select the mail template from which to load the content and to

do other mail template management tasks. After loading the contents
from a mail template, editing the content in the mail activity will affect
only the mail activity, not the template.

Subject

Provides a description of the activity to the recipient of the mail
notification.

Plaintext body

Provides additional details to the recipient that describe the outcome of
the activity, in plaintext format. For example, an account or access
request was approved.

XHTML body

Provides additional details to the recipient that describe the outcome of
the activity, in XHTML format. For example, an account or access
request was denied.

7. When the fields are complete, click **OK**.

8. Click other tabs to specify additional information. Then, either click **OK** to save
the changes or **Apply** to save your changes and continue.

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

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, as a System Administrator you can enable and
configure it in the Administrative console.

To customize checkout, you must define a global operation to be executed during
check-out. 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 you how to define a
checkout operation with or without RFI node followed by the checkout extension.

Note: Checkout operation customization is not applicable for automatic check-in
and check-out with Privileged Access Agent or Privileged Session Gateway.

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 you are
   configuring the credential default settings.
   You are prompted to open the Java Web start file.

4. Open the file with the Java Web Start Launcher and click **OK**.

5. In the **Operation Diagram**, click **Properties**.

6. In the Properties window, under **Input Parameters**, add the relevant data in the table below for credential, credential lease, account and person then click **OK**.

	ID	Type
	credential	Credential
	credentialLease	CredentialLease
S: Subject	account	Account
R: Requestee	lessee	Person

7. Add an **Extension** node in the Operation Diagram.
8. Right-click the **Extension** node and select **Properties**.
9. In **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.

10. Click **Save**.
11. From the Administrative console, select **Manage Shared Access** > **Configure Credential Default Settings**.
12. 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 199, 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 `CustomLables.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 `CO` instead of `CP` and save the entry. The label for process type `CO` is defined in `Labels.properties` `processType.CO`

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

Chapter 13. Activity administration

You can manage your activities to view your activities, approve and reject requests, and complete work order activities. You can provide information for a request to proceed, approve and reject recertification requests, complete compliance alerts, and delegate activities to other users.

Use the View Activities page to lock, unlock, forward, and respond to action items.

Use the View Activities by User page to view and complete items for other users.

Use the Delegate Activities page to delegate activities to another user when you are not available to manage them.

System administrators can view and respond to all user activity lists. However, system administrators cannot lock work items unless they meet the criteria of being a potential owner of the item.

Activities

An activity is an action item that occurs in your to-do list as part of a workflow process and requires your action. The types of activities are approval requests, work order requests, requests for information, compliance alerts, and recertifications.

Activities are created by requests from other users that require additional information, approval of a request, or for completion of a task. Requests for these users occur as activities for the person who does the action. These activities must be completed for the request to be completed. In some cases, requests are sent to multiple participants who are authorized to complete them.

If you do not complete an activity in the allotted amount of time, it might escalate to another user.

You can also delegate all of your activities for a specified period, if you are unavailable for that time.

Approval activities

An approval activity occurs in the activities list of the user who is prompted to approve or reject a request. Approval activities in your activities list are part of workflow processes that require your response before they can be completed.

If the request is approved, the next activity in the workflow is processed. If, however, the request is rejected, the workflow stops and no additional activities are processed.

If you submit a request that must be approved, the approval activity is sent to all participants in the assigned group except to the user who makes the request. You might be a member of the group who normally approves requests. If you are the person who makes the request, you do not see the approval activity in your activities list.

If a timeout occurs, the Activity Result Summary Code is set to SF (failed). If a participant resolution failure occurs, the Activity Result Summary Code can take the following values:

AA (approved)
> If the request is submitted by the system administrator, the request is automatically approved by the system administrator. The approval occurs even though the system administrator is not explicitly set as an escalation participant. The result is set to Approved.

SF (failed)
> The Approval activity ends with result set to Failed, if:
> - The request is submitted by a non-admin user.
> - The escalation participant is not defined at all.
>
>   **Note:** This result is true even when the requester is the system administrator.
> - The participant resolution failed.

If the property enrole.workflow.skipapprovalforrequester is set to true in enRole.properties file and the requester is identified as one of the participant users, the approval is completely skipped. The Activity Result Summary Code is set to AA (approved). When an RFI activity times out or fails because of participant resolution failure, the Activity Result Summary Code is set to SF (failed) for both cases.

Approval states

When you view the status of an approval, the approval activity is in one of several states.

The states of an approval activity can be viewed only by the user who submitted the request. Table 26 describes each approval activity state.

Table 26. 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 27. 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 ManagerIBM 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 28 on page 206 gives a description of each work order state.

Table 28. 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**.

Delegation Schedule

When you are not available to manage your activities, you can delegate them to another authorized user. You can setup multiple delegation periods as long as they do not overlap.

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. If you are delegating activities for yourself, you must have both read and write Delegate access control item attribute permissions set to Grant.

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 to other users. You can setup multiple delegation schedules for multiple delegates but the time periods cannot overlap. 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 14. Requests administration

The View Requests task indicates the progress and completion of submitted changes and requests that you and other users make to the system.

Request status is available through the View Requests task from the main navigation tree. You can choose to filter your search for requests by user or service. To view pending requests, click **View Requests** > **View Pending Requests by User** or **View Requests** > **View Pending Requests by Service**. You can also choose to view the status of all pending and completed requests from the **View Requests** > **View All Requests** task.

Requests

Requests are items that initiate a workflow, or work order for manual service operations, and instigate the various activities of a workflow.

There are many different types of requests that can occur, such as requesting changes to accounts, adding and modifying users, and changing policies. Some requests might require the completion of a to-do activity by another user, such as an approval or recertification. Other requests might complete without any action required.

Note: Requests that do not initiate a workflow, such as Orphan Account Requests do not get displayed in the pending or completed requests.

Requests can involve several steps to complete. Each step might require different users to complete an action. You can view the status of a request by viewing pending requests or all requests that are both pending and completed.

Completed requests are requests that completed processing. The completion of a request does not mean that it was successful. Requests might fail, might complete with a warning message, or might be canceled while in a pending state.

Pending requests are requests that are submitted but are not finished. These requests might be in the process of running or might require the completion of a workflow activity, such as a recertification or approval activity.

Request states

When you view the status of a request, the request might be in one of several states.

The states of a request can be viewed only by the user who submitted the request. The following table provides a description of each request state.

Table 29. 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 29. 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 the parent and the 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 child request fail 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 fail. 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**.

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 from Privileged Access Agent. 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.

Management Activity Report
> This report shows various administrator activities and the details of each activity, such as event category, resource, entity type, and identity provider name.

Check-In Check-Out Activity Per Resource Report
> This report shows the details of check-in check-out activities under selected resources, such as number of checkouts, number of privileged users, and number of credentials.

Check-In Check-Out Activity History Report
This report shows the list of check-in and check-out activities on credentials.

Check-In Check-Out Activity Per Credential Report
This report shows the check-in and check-out activities related to selected credentials.

Check-In Check-Out Activity Per Resource and Privileged User Report
This report shows the check-in and check-out activities based on selected resources and privileged user names.

Privileged Session Gateway Access History Report
This report shows a list of Privileged Session Gateway access history.

For more information about these reports, see "Report descriptions and parameters."

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 scheduled 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 227.

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 Analytics" on page 231.

Note:
- You must map the attributes to the entities before you work with the IBM Cognos shared access reports. .
- 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 30. 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 31. Filters for the Application Instance Activity 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.
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 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 32. 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	Displays the credential.

Parameter	Description
Credential Pool Service Business Unit	Displays the business unit that is associated with the credential pool service.
Credential Pool Service	Displays the service information that has the credential pool entitlements that are associated with it.
Credential Pool Owner Type	Displays the credential pool owner type.
Credential Pool Owner	Displays the credential pool owner.
Credential Pool	Displays the credential.

See "Generating the report through IBM Cognos Analytics" on page 231.

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 33. 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 Analytics" on page 231.

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 34. Filters for the Shared Access Entitlement Definition Report

Parameter	Description
Business Unit	Displays the business unit that is associated with the credential service.
Service	Displays the service of the Privileged ID.
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 Analytics" on page 231.

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 35. Filters for Shared Access History Report

Parameter	Description
Start Date	Displays all events from the specified date.
End Date	Displays all events until the specified date.
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.
Audit of	Displays the entitlement types for which an audit is performed. For example, credential, or credential pool.
Credential	Displays the credential.
Credential Pool Owner Type	Displays the type of the credential owner. The type of owner can be either a person or a role.
Credential Pool Owner	Displays the credential owner name. The owner name can be either a person name or a role name.
Credential Pool	Displays the credential pool.

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 from Privileged Access Agent. 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 Privileged Access Agent.

The following table describes the parameters for filtering the report.

Table 36. 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.

Parameter	Description
User Machine IP Address	Displays the unique identifier of the machine that is used by the Privileged Access Agent user.
Privileged ID	Displays the credential.
Audit Event	Displays the action that is performed on the 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 Analytics" on page 231.

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 37. 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 Analytics" on page 231.

Management Activity Report

This report shows various administrator activities and the details of each activity, such as event category, resource, entity type, and identity provider name.

Table 38. Filters for the Management Activity Report

Parameter	Description
Start Date	Displays all events from the specified date.
End Date	Displays all events until the specified date.
Business Unit	The name of the business unit.
Administrator Name	Name of the administrator
Event Category	Displays the list of events that are available. **Note:** If **Life Cycle rule** is selected, the **Business Unit** parameter shows **Not applicable**.
Action	Displays the list of actions that are available.
Resource	Name of the resource.
Entity Name	Displays the name of the entity.
Result	Displays the result. For example, **Success**, **Fail**, or **Pending**.

Check-in and Check-out Activity per Resource Report

This report shows the details of check-in check-out activities under selected resources, such as number of checkouts, number of privileged users, and number of credentials.

Note: If the data is captured before IBM Security Privileged Identity Manager version 2.0.2 Fix Pack 6, the **Business Unit** data is shown as **Not Applicable** in the report

Table 39. Filters for the Check-In Check-Out Activity Per Resource Report

Parameter	Description
Date Range: Start Date	Displays all events from the specified date.
Date Range: End Date	Displays all events until the specified date.
Business Unit	The name of the business unit.
Resource	Displays all the resources that are associated with the credential.

Check-in and Check-out Activity History Report

This report shows the list of check-in and check-out activities on credentials.

Note: If the data is captured before IBM Security Privileged Identity Manager version 2.0.2 Fix Pack 6, the **Business Unit** data is shown as **Not Applicable** in the report

Table 40. Filters for the Check-In Check-Out Activity History Report

Parameter	Description
Check-out Date Range: Start Date	Displays all events from the specified date.
Check-out Date Range: End Date	Displays all events until the specified date.
Business Unit	The name of the business unit.
Resource	Displays all the resources that are associated with the credential.

Parameter	Description
Credential Name	Displays all the credentials that are associated to the activity.
Checked Out By	Displays the list of users that checked out a credential.
Checked In By	Displays the list of users that checked in a credential.
Is Credential Checked In?	Displays the list of options to determine whether a credential is checked in.
Credential Type	Displays the type of credential that is checked out.

Check-in and Check-out Activity per Credential Report

This report shows the check-in and check-out activities related to selected credentials.

Note: If the data is captured before IBM Security Privileged Identity Manager version 2.0.2 Fix Pack 6, the **Business Unit** data is shown as **Not Applicable** in the report

Table 41. Filters for the Check-In Check-Out Activity Per Credential Report

Parameter	Description
Date Range: Start Date	Displays all events from the specified date.
Date Range: End Date	Displays all events until the specified date.
Business Unit	The name of the business unit.
Resource	Displays all the resources that are associated with the credential.
Credential Name	Displays all the credentials that are associated to the activity.

Check-in and Check-out Activity per Resource and Privileged User Report

This report shows the check-in and check-out activities based on selected resources and privileged user names.

Note: If the data is captured before IBM Security Privileged Identity Manager version 2.0.2 Fix Pack 6, the **Business Unit** data is shown as **Not Applicable** in the report

Table 42. Filters for the Check-In Check-Out Activity Per Resource and Privileged User Report

Parameter	Description
Date Range: Start Date	Displays all events from the specified date.
Date Range: End Date	Displays all events until the specified date.
Business Unit	The name of the business unit..
Resource	Displays the name of the resource.
Privileged User Name	Displays the name of the privileged user.

Privileged Session Gateway Access History Report

This report shows a list of Privileged Session Gateway access history.

Table 43. Filters for the Privileged Session Gateway Access History Report

Parameter	Description
Session start date range: Start date	Displays all Privileged Session Gateway access events from the specified date.
Session start date range: End date	Displays all Privileged Session Gateway access events until the specified date.
Privileged User Name	The names of the privileged users that are associated with the session.
Business Unit	The name of the business unit.
Resource	Displays all the resources that are associated with the session.
Target Address	Displays the host that the privileged user is connecting to.
Credential Type	Displays the type of credential. For example, password or SSH Key.

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.

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 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**.

Generating the report through IBM Cognos Analytics

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 Analytics.
2. Select the report model **ISPIMReportingModel**.
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 is a link to an external web application. It is defined by a unique identifier, a URL, and optional parameters. The task can be associated with IBM Security Privileged Identity Manager views. 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 = Tâche Personnalisée`.

6. Type the URL that links to your custom task.
7. Optional: Type the URL that links to the image you want to display on the task card.
8. Optional: Specify a menu category for the header.
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 Personnalisée`.
7. Optional: Create or change custom task parameters.
   a. In the **Task Parameters** table, click **Create** or select a parameter and click **Change**.
   b. Specify a parameter name.
   c. Specify a parameter value
   d. Click **OK**.
8. Optional: Delete custom task parameters.
   a. In the **Task Parameters** table, select one or more parameters and click **Delete**.
   b. On the Confirm page, ensure that the parameters are the ones you want to delete, and then click **Delete**.

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

What to do next

Log in to the 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.

Console setup for users

As a Privileged Identity Manager Administrator, grant Privileged Administrators and Privileged Users, access to the appropriate consoles from the administrative console.

Tip: After IBM Security Privileged Identity Manager installation is complete, to grant access for the first time, in the virtual appliance dashboard, in the **Quick Links** widget, click **Identity and Credential Vault Administration**. This link launches the administrative console. Log on with the `pim manager` credential to complete the following first steps.

If not already created, create some users manually. For example, see "Creating user profiles" on page 25.

Note: For advanced user onboarding strategies in production environments, however, consider using features such as CSV bulk upload, REST APIs, external user registries, or integration with IBM Security Identity Manager.

Table 44. Granting users access to the consoles

Persona	Consoles	Requirements	Steps to grant access
Privileged Administrator	Service Center	• Admin Domain administrator privileges • Privileged Administrator group member	1. Make the user an administrator of an Admin Domain. 2. Add the user to the Privileged Administrator group.
	Administrative console	Privileged Administrator group member	Add the user to the Privileged Administrator group.
Privileged User	Self-service console	Privileged User group member	1. Verify that the users you onboard are already members of the Privileged User group. If required, add the users to the Privileged User group. 2. Transfer users into the Admin Domain. For example: `JKE Datacenter A`
Security Auditor	Privileged Session Recorder console	Session Recorder Auditor group member	Add the user to the Session Recorder Auditor group.
Privileged Administrator	Single Sign-On console	-	-
Security Auditor	Reporting	-	Grant required auditors or users access to reports.

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 45. Default access control items for Shared Access Module

Protection category	Name	Type	Principal
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
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

Protection category	Name	Type	Principal
Credential Pool	Default ACI for Credential Pool: Grant Search for Everyone	erCredentialPool	Everyone
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant Search to Auditor Group	Dynamic role	Auditor Group
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant Search to everyone	Dynamic role	Everyone
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant All to Supervisor/Domain Admin/Sponsor	Dynamic role	Supervisor Domain Admin Sponsor
Resource	Default ACI for Credential Service: Grant All to Domain Admin	erCVService	Domain Admin
Static Organizational Role	Default ACI for Org Role: Grant All to Supervisor/Domain Admin/Sponsor	Organizational Role	Supervisor Domain Admin Sponsor
Static Organizational Role	Default ACI for Org Role: Grant Search for everyone	Organizational Role	Everyone
Static Organizational Role	Default ACI for Org Role: Grant Search to Help Desk/Auditor Groups	Organizational Role	Help Desk Auditor Groups
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 12 on page 71.

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 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 46. 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 47. 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 48. 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 CenterIdentity 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 239.

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 239.

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 239.

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 239.

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**.

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 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 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 25.

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 46
   - "Administrative domains" on page 45

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.

Adding credentials with the administrative console

As a Privileged Administrator, you can add credentials of managed resources into the credential vault.

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 239.

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:

      Sharing options

         Select one of the following settings:

Use default setting
> If you want to use the default settings for your system for sharing credentials, select this option.

One user at a time
> If you want to share the credential exclusively, select this option. Users must check out the credential to use it. If you select this option, only one user at a time can check out the credential.

Multiple users or applications
> Select this option to share the credential non-exclusively or enable the credential for use in applications.
>
> **Note:** If this option is selected, users are not required to check out the credential to use it.

No sharing
> The credential is stored in the credential vault but it is not shared. privileged users are not able to access the credential.

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.

   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 Privileged Access Agent for automatic checkout. The resource alias is the IP address or hostname of the managed resource to which the credential applies. Privileged Access Agent 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 check in and check out process for shared IDs.

Change password or key upon check in:
Specify if the credential password or key must be changed upon check in.

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
Specify the operation for checking out credentials.

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.

Allow view password or key download to user
Select the check box if you want to display the credential password or allow key download to the user on the Self-service console.

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 265.

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 239.

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 280.

   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 239.

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 280.

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 Privileged Access Agent for automatic checkout. The resource alias is the IP address or hostname of the managed resource to which the credential applies. Privileged Access Agent 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.

   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 Check-in and Check-out 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 Check-in and Check-out 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. Select the **Change password or key upon check in** check box if you want the password or key to be changed on the account and the managed resource when the user checks in the credential.

   c. Specify the number of hours, days, or weeks in the **Maximum check-out duration** field for which the credential can be checked out

d. Select the **Enable check out search** check box if you want to enable the credentials for a check-out search.

e. Select the **Allow view password or key download to user** check box if you want the credential password and key to be visible to the user on the Self-service console.

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 239.

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 280.

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**.

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 239.

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 280.

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" on page 280.

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. After you check in a credential, any existing Privileged Session Gateway sessions that are associated with the credential are terminated.

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

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® 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".

IBM ®

Printed in USA