IBM Security Identity Manager
Version 6.0.0.10

Scenarios Topics

IBM

IBM Security Identity Manager
Version 6.0.0.10

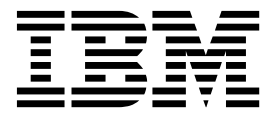*Scenarios Topics*

IBM

Table of contents

Table list

v

Chapter 1. Scenarios overview

The following scenarios describe some of the common activities that users and administrators do in IBM® Security Identity Manager to configure the environment and complete daily tasks.

The company, for the purposes of these scenarios, is a large public insurance company. Employees at the company have a wide variety of roles, from accounting to adjusting claims, to customer service. The company grew both organically and through acquisitions over time. As a result, the company has many fragmented information technology systems and processes for managing its business.

In some cases, these systems are used by only a few individuals or they are dependent on employee responsibilities. For example, accountants use a proprietary accounting software developed internally.

Customer service representatives use a customer relations management (CRM) system that was developed and serviced by a third party. Other systems, such as email and voice mail, are common to all employees.

Internal policies are in place to control access to these resources. For example, customer service representatives are not allowed access to accounting software. These policies are difficult to manage and control, requiring approval forms or email tag.

When employees switch departments and jobs, significant time can pass before the employee is removed from old systems and added to new systems. The delays create security issues and decrease productivity.

The need to control access to resources also places a burden on the insurance company management. Managers provide approvals for subordinates who need new access to resources, remove access in some circumstances, and regularly audit those resources for accounting purposes. Away from the office or on vacation, managers often have no way to delegate approvals to other individuals. They must keep records of such delegation in the form of paper or email.

Because it is a large public company, it is also required to follow many securities regulations and must make regular internal audits. Audit reports are time consuming and done manually, often once or twice a year at considerable expense.

Because of the expense and loss of productivity in managing this complex environment, the insurance company decided to implement IBM Security Identity Manager.

The scenarios in this section demonstrate how company employees would use IBM Security Identity Manager to provision employees into an identity system and do common identity management activities. These scenarios are grouped by the type of user who does the activity. Out of the box, IBM Security Identity Manager provides views for these five common user types:

- System administrator

  This person is responsible for IBM Security Identity Manager setup and administration activities. Activities include provisioning people, adding services,

defining access entitlements, and setting permissions for system users. In most organizations, these administrative tasks are assigned to different users with different roles, permissions, and responsibilities. For the purposes of these scenarios, these administrative tasks are done by one person.

- Service owner

  This person is responsible for enabling users to do tasks associated with services and access entitlements.

- Help desk

  This person is responsible for assisting users with common user and account management tasks, such as locked accounts and passwords.

- Manager

  This person is responsible for users who report to them.

- Auditor

  This person is responsible for auditing the system by creating reports.

- Non-administrative user

  This person is a common user of resources whose identity is managed by IBM Security Identity Manager.

The scenarios are just a subset of activities that these user types do, but they highlight some of the capabilities that IBM Security Identity Manager offers.

Chapter 2. Administrative scenarios

These scenarios demonstrate some of the advanced tasks that users with administrative roles would do to set up IBM Security Identity Manager for a production environment.

First, obtain a system administrator user ID (initially *itim manager*) and password (which is initially *secret*).

People and IBM Security Identity Manager account provisioning

This scenario demonstrates how to automatically provision people and create IBM Security Identity Manager accounts that use a DSML v2 feed.

In order for the insurance company to use IBM Security Identity Manager, it must first have identities to manage. This task is done by feeding information about people (identity records) into the system. During the initial setup of the environment, a IBM Security Identity Manager administrator setup these identity feeds. This task might also be relegated to a service owner who manages the HR systems.

For the purposes of this scenario, the HR service owner provides a directory services markup language (DSML) file to a IBM Security Identity Manager administrator.

Providing a DSML file is one way to provision people and accounts in IBM Security Identity Manager. There are several other ways to provision people and other objects. For example, provisioning might use the manual creation and population of users from **Manage Users** in the IBM Security Identity Manager navigation tree.

Creating a DSML feed file

The first step is to create a sample DSML feed file, which contains information about different users to be populated in this system.

Before you begin

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

About this task

The insurance company uses an HR system to store its employee directory. To populate the IBM Security Identity Manager system, the HR system outputted this content into a Directory Services Markup Language (DSML) file. This file format allows the administrator to populate initial content and to make subsequent changes to the content of the Security Identity Manager people registry.

In many cases, this employee information is stored in one or more IT systems, such as Windows Active Directory or LDAP. Business partner records and employee

records often have separate HR systems. Security Identity Managerenables management of these disparate systems and import identity records from many different sources.

Using DSML to populate identity records in this scenario simplifies the creation of users who are later responsible for actions in subsequent scenarios.

This DSML file contains the names of the following sample users:

Judith User
　　Judith User is a regular employee who requires access and accounts on resources in order to do work.

Chuck Manager
　　Chuck Manager is Judith User's manager and has some management control over access to resources.

Mike Sysadmin
　　Mike Sysadmin is a Security Identity Manager administrator. Administrator responsibilities are to set up and administer the identity management system.

James Owner
　　James Owner is a service owner, and controls specific system resources in Security Identity Manager.

Janice Helpdesk
　　Janice Helpdesk is a standard help desk assistant who serves a help function in Security Identity Manager. In this case, the help desk function is to verify user identities and to change user passwords that are lost or forgotten.

Jeff Auditor
　　Jeff Auditor is an auditor whose job it is to create audit reports.

Create and save this DSML feed file as `feedfile.dsml` with a text editor. Each entry in the file contains personal, business, and contact information about each user.

```
<dsml><directory-entries>
<entry dn="uid=juser">
<objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
<attr name="givenname"><value>Judith</value></attr>
<attr name="initials"><value>JU</value></attr>
<attr name="mobile"><value>(555) 555-0100</value></attr>
<attr name="roomnumber"><value>R1-100</value></attr>
<attr name="homephone"><value>(555) 555-0199</value></attr>
<attr name="pager"><value>(555) 000-1111</value></attr>
<attr name="sn"><value>User</value></attr>
<attr name="cn"><value>Judith User</value></attr>
<attr name="title"><value>Standard Employee</value></attr>
<attr name="telephonenumber"><value>(555) 555-0100</value></attr>
<attr name="postaladdress"><value>111 Fictional Pl, New York, NY  55555</value></attr>
<attr name="erAliases"><value>juser</value></attr>
</entry>

<entry dn="uid=cmanager">
<objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
<attr name="givenname"><value>Chuck</value></attr>
<attr name="initials"><value>CM</value></attr>
<attr name="mobile"><value>(555) 555-0100</value></attr>
<attr name="roomnumber"><value>R1-101</value></attr>
<attr name="homephone"><value>(555) 555-0199</value></attr>
<attr name="pager"><value>(555) 000-1111</value></attr>
<attr name="sn"><value>Manager</value></attr>
<attr name="cn"><value>Chuck Manager</value></attr>
<attr name="title"><value>Manager</value></attr>
<attr name="telephonenumber"><value>(555) 555-0100</value></attr>
<attr name="postaladdress"><value>111 Fictional Pl, New York, NY  55555</value></attr>
```

```
              <attr name="erAliases"><value>cmanager</value></attr>
              </entry>

              <entry dn="uid=msysadmin">
              <objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
              <attr name="givenname"><value>Mike</value></attr>
              <attr name="initials"><value>MS</value></attr>
              <attr name="mobile"><value>(555) 555-0100</value></attr>
              <attr name="roomnumber"><value>R1-102</value></attr>
              <attr name="homephone"><value>(555) 555-0199</value></attr>
              <attr name="pager"><value>(555) 000-1111</value></attr>
              <attr name="sn"><value>Sysadmin</value></attr>
              <attr name="cn"><value>Mike Sysadmin</value></attr>
              <attr name="title"><value>Administrator</value></attr>
              <attr name="telephonenumber"><value>(555) 555-0100</value></attr>
              <attr name="postaladdress"><value>111 Fictional Pl, New York, NY  55555</value></attr>
              <attr name="erRoles"><value>ITIM Administrators</value><value>Employee</value></attr>
              <attr name="erAliases"><value>msysadmin</value></attr>
              </entry>

              <entry dn="uid=jowner">
              <objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
              <attr name="givenname"><value>James</value></attr>
              <attr name="initials"><value>JO</value></attr>
              <attr name="mobile"><value>(555) 555-0100</value></attr>
              <attr name="roomnumber"><value>R1-103</value></attr>
              <attr name="homephone"><value>(555) 555-0199</value></attr>
              <attr name="pager"><value>(555) 000-1111</value></attr>
              <attr name="sn"><value>Owner</value></attr>
              <attr name="cn"><value>James Owner</value></attr>
              <attr name="title"><value>Service Owner</value></attr>
              <attr name="telephonenumber"><value>(555) 555-0100</value></attr>
              <attr name="postaladdress"><value>111 Fictional Pl, New York, NY  55555</value></attr>
              <attr name="erAliases"><value>jowner</value></attr>
              </entry>

              <entry dn="uid=jhelpdesk">
              <objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
              <attr name="givenname"><value>Janice</value></attr>
              <attr name="initials"><value>JH</value></attr>
              <attr name="mobile"><value>(555) 555-0100</value></attr>
              <attr name="roomnumber"><value>R1-104</value></attr>
              <attr name="homephone"><value>(555) 555-0199</value></attr>
              <attr name="pager"><value>(555) 000-1111</value></attr>
              <attr name="sn"><value>Helpdesk</value></attr>
              <attr name="cn"><value>Janice Helpdesk</value></attr>
              <attr name="title"><value>Help Desk</value></attr>
              <attr name="telephonenumber"><value>(555) 555-0100</value></attr>
              <attr name="postaladdress"><value>111 Fictional Pl, New York, NY  55555</value></attr>
              <attr name="erAliases"><value>jhelpdesk</value></attr>
              </entry>

              <entry dn="uid=jauditor">
              <objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
              <attr name="givenname"><value>Jeff</value></attr>
              <attr name="initials"><value>JA</value></attr>
              <attr name="mobile"><value>(555) 555-0100</value></attr>
              <attr name="roomnumber"><value>R1-105</value></attr>
              <attr name="homephone"><value>(555) 555-0199</value></attr>
              <attr name="pager"><value>(555) 000-1111</value></attr>
              <attr name="sn"><value>Auditor</value></attr>
              <attr name="cn"><value>Jeff Auditor</value></attr>
              <attr name="title"><value>Auditor</value></attr>
              <attr name="telephonenumber"><value>(555) 555-0100</value></attr>
              <attr name="postaladdress"><value>111 Fictional Pl, New York, NY  55555</value></attr>
              <attr name="erAliases"><value>jauditor</value></attr>
              </entry>

              </directory-entries>
              </dsml>
```

Creating a DSML service

The next step is to create a DSML service.

Before you begin

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

First, log on to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

To import identity records into Security Identity Manager by using DSML, a Security Identity Manager administrator must first create a DSML identity feed service. In Security Identity Manager, a service represents a managed resource, such as an operating system, a database application, or another application that Security Identity Manager manages. With a DSML service, the service represents the idea of a user repository. After this service is established, users are not automatically populated into the system; a reconciliation must be run. However, the service can be tested to ensure that the file is in the system.

To create a DSML service in Security Identity Manager, complete these steps:

Procedure

1. Log on to the administrative console as an administrator.
2. From the navigation tree, click **Manage Services**.
3. On the Select a Service page, click **Create**.
4. On the Select the Type of Service page, select the **DSML identity feed** service type.
5. Click **Next** to display the Service Information page.
6. On the Service Information page, complete these steps:
   a. In the **Service name** field, type `DSML Feed`.
   b. Optional: Provide a description, user ID, and password for the service name.
   c. In the **File name** field, type the path name of the DSML file you saved and stored on the IBM Security Identity Manager Server. For example, `C:\feedfile.dsml`.

      Note: For Linux, determine whether permissions are set to `644` on the DSML file for the reconciliation operation to work.
   d. Select the **Use workflow** check box.
   e. Select the **Evaluate separation of duty policy when workflow is used** check box.
   f. Leave the **Placement rule** field blank. If you want to enter a placement rule, see "Determining the placement of the person" in the *Configuration Guide* in the IBM Security Identity Manager product documentation website at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0.0.2/kc-homepage.htm.
   g. Click **Test Connection** to confirm you can connect to the service.
   h. Click **Finish**.
7. On the Success page, click **Close**.
8. On the Select a Service page, click **Close**.

Modifying the default provisioning policy for IBM Security Identity Manager

The next step is to modify the default provisioning policy for IBM Security Identity Manager.

Before you begin

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

You must first be logged on to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

A provisioning policy grants access to one or more managed resources. You can use provisioning policies to define or set required attributes. In this task, the IBM Security Identity Manager administrator sets up a provisioning policy. This action automates the provisioning of users into the system when the DSML feed is reconciled. It provides users with a standard password so that they can log on later to do tasks related to their user type. This process is a simplified example of how Security Identity Manager fits into an HR on-boarding process.

To modify the default provisioning policy for the Security Identity Manager service, complete these steps:

Procedure

1. Log on to the administrative console as an administrator.
2. From the navigation tree, click **Manage Policies** > **Manage Provisioning Policies**.
3. On the Manage Provisioning Policy page, click **Search**. A list of all provisioning policies is shown.
4. In the **Provisioning Policies** table, click **Default provisioning policy for ITIM**.
5. On the General notebook page, ensure that the policy status is set to **Enable**. Click the **Entitlements** tab.
6. On the Entitlements notebook page, complete these steps:
   a. Ensure that there is an entitlement named `ITIM Service` with a target type of `Specific Service` and a provision option of `Automatic`. If the provisioning option is set to `Manual`, a user account cannot be created when the DSML feed is reconciled and people are populated into the system.
   b. Check the box next to `ITIM Service` and click **Parameters**.
7. On the Entitlement Parameter page, click **Create**.
8. On the Add New Parameter page, go to the attribute table page, check the box next to **Password** and click **Continue**.
9. On the Define Constant page, type `secret` as the password and click **Continue**. This procedure sets the default password of *secret* for all users provisioned to **ITIM Service**. In a production environment, do not create a standard password for all users in a provisioning policy. It creates security vulnerabilities.

10. On the Entitlement Parameter page, click **Continue**.
11. On the Entitlements notebook page, click **Submit**.
12. On the Schedule page, click **Submit**.
13. On the Success page, click **Close**.

Setting password security properties

The next step is to set password security properties for users to be added.

Before you begin

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

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

Security Identity Manager administrators often set security policies in line with company policy. Some companies require passwords to be regularly reset and sent by email to employees; other companies might allow the user to change their password. Password synchronization can be set to allow a common password to be used on multiple IT resources. However, this solution might not be feasible if different corporate IT systems have different security settings or policies.

To set security properties in Security Identity Manager, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Set System Security** > **Set Security Properties**.
3. On the Set Security Properties page, complete these steps:
   a. Select the check box next to **Enable password editing** if not checked.
   b. Select the check box next to **Enable password synchronization** if not checked.
   c. Select the check box next to **Set password on user during user creation** if not checked.
   d. Click **OK**.

Reconciling the DSML service and loading users into IBM Security Identity Manager

Next, reconcile the DSML service, which adds people and Security Identity Manager user accounts to the system with the modified provisioning policy.

Before you begin

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

First, log on to the Security Identity Manager administrative console as `itim manager`.

About this task

After the provisioning settings are in place, the Security Identity Manager administrator can proceed to load identity records into the system. Reconciliation copies information out of the DSML file into the Security Identity Manager data store and run policies. In this example, the process creates the identity records and creates an Security Identity Manager service account for each user.

An Security Identity Manager service account allows a user to log in to the Security Identity Manager and do tasks. For example, the user might request an account. Some people might not require an Security Identity Manager service account. For example, an external customer or IBM Business Partner who requires access to a specific managed resource might not require an Security Identity Manager account. However, the customer or IBM Business Partner might be populated into the system as a person.

To reconcile the DSML service and populate users, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Manage Services**.
3. On the Select a Service page, complete these steps:
   a. In the **Search information** field, type DSML and click **Search**.
   b. In the **Services** table, click the icon (▶) next to **DSML Feed** and click **Reconcile Now**.
4. On the Success page, click **Close**, or verify that the reconciliation operation is successful.

Results

If the reconciliation operation is successful, the users in the feed file are created. Each user has an account on the ITIM Service with a password of secret.

What to do next

To verify that the operation is successful, complete one of the following steps:
- Click **View my request** to display recent requests. Refresh the **Requests** table until the Reconciliation task shows a status of Success.

   Note: On the system with Microsoft SQL database, the view might show the *Pending* state when the task is completed. You must cancel the pending task and run the reconciliation again to successfully finish the task.
- In the left navigation pane, click **Manage Users**, and then search to view the added users.

Assigning a manager to a user

The next step is to assign a manager to a user.

Before you begin

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

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

Chuck Manager is a controller who manages of a team of accountants, among them Judith User, who is team lead. To do approvals and other management-related activities in Security Identity Manager, Chuck must first be recognized in the system as the manager of Judith. Often, this assignment is done ahead of time by an HR system. The data is stored in a user repository such as LDAP, Active Directory, or an identity feed file. This task shows how users can be managed through the Security Identity Manager interface. The task shows how to define a manager for a user, enabling additional manager-related scenarios.

To assign a manager to a user, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Manage Users**.
3. On the Select a User page, complete these steps:
   a. In the **Search information** field, type `Judith User`, select `Full Name` in the **Search by** field and click **Search**.
   b. In the **Users** table, click the name of the user Judith User.
4. On the Personal Information notebook page, click the **Business Information** tab.
5. On the Business Information notebook page, click the **Search** button next to **Manager**.
6. On the Select People page, complete these steps:
   a. Type `Chuck Manager` in the **Value** field and click **Search**.
   b. Select the radio button next to the user Chuck Manager and click **OK**.
7. On the Business Information notebook page, click **Submit Now**.
8. On the Success page, click **Close**.
9. On the Select a User page, click **Close**.

Assigning users to IBM Security Identity Manager default groups

The next step is to assign users to IBM Security Identity Manager groups.

Before you begin

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

You must first be logged on to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

Groups provide a way to manage what tasks can be done by a specific user in IBM Security Identity Manager. Groups use views to control what tasks are available. You can create your own views, create a group that has those views defined, and

assign users to the group. Users can be assigned to more than one group. For new groups, you also need to set permissions through access control items. IBM Security Identity Manager comes with five default groups: Manager, System Administrator, Service Owner, Help Desk Assistant, and Auditor.

While a IBM Security Identity Manager administrator might initially set up and assign users to the default groups, a help desk or service owner often does this work.

Users in this scenario are assigned to the following default groups:

Table 1. Scenario users and their assigned group

User	Group
Chuck Manager	Manager
Mike Sysadmin	System Administrator
James Owner	Service Owner
Janice Helpdesk	Help Desk Assistant
Jeff Auditor	Auditor
Vic PrivAdmin	Privileged Administrator
Jane PrivUser	Privileged User

To assign the user Chuck Manager to a group, for example, complete these steps:

Procedure

1. Log on to the administrative console as an administrator.
2. From the navigation tree, click **Manage Groups**. The Select a Service page opens.
3. On the Select a Service page, complete these steps:
   a. In the **Search information** field, type `ITIM Service`.
   b. In the **Search by** field, specify that you want to search against services.
   c. Select **ITIM** from the Search type list and then click **Search**. **ITIM Service** is shown.
   d. In the Services table, select **ITIM Service** and then click **Continue**. The Select Group page opens.
4. On the Select Group page, complete these steps to view the groups that exist for **ITIM Service**:
   a. In the **Search information** field, type `Manager`.
   b. In the **Search by** field, specify to search against group names or descriptions and click **Search**. The search result is shown.
   c. In the **Groups** table, click the icon ( ) next to **Manager** and click **Add Members**.
5. On the Add Members page, complete these steps:
   a. In the **System account information** field, type `Chuck Manager` and click **Search**.
   b. Mark the check box next to the user Chuck Manager and click **OK**.
6. On the Confirm page, click **Submit**.
7. On the Success page, click the link next to **Return to the list of groups I was working with**.

8. Repeat these steps for the other users and assign them to their respective groups as provided in the table.

Verifying user login

The next step in this scenario is to verify that the IBM Security Identity Manager users can log in.

About this task

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

The Security Identity Manager administrator populates users and defines their user views. Then, the administrator does a login test to ensure that each user can log in and has access to the appropriate views and tasks.

Verify the login for the following users in Security Identity Manager as shown in the table:

Table 2. Users and their Security Identity Manager user IDs

Name	Security Identity Manager User ID
Judith User	*juser* (use self-care or Identity Service Center interface only)
Chuck Manager	*cmanager*
Mike Sysadmin	*msysadmin*
James Owner	*jowner*
Janice Helpdesk	*jhelpdesk*
Jeff Auditor	*jauditor*

The user Judith User can log in to the self-care or Identity Service Center user interface. However, an error occurs if you attempt to log in to the administrative console user interface. Use the self-care or Identity Service Center user interface login address to log Judith in to Security Identity Manager.

To verify that a user can log in, complete these steps:

Procedure

1. From the navigation tree, click **Log Out** as administrator.
2. On the Login page for the user, in the **User ID** field, type `juser` and, in the **Password** field, type `secret`. Click **Log In**.

   This user ID is provided in the **Identity Manager login ID** field in the new user's Personal Information page.
3. If you cannot log in as a user, log in as an administrator. From the navigation tree, click **Manage Users** to check on the existence of users, Security Identity Manager user accounts, and passwords.
4. If forgotten password questions are enabled, the Specify Forgotten Password Information page prompts you for the forgotten password information. Optionally, type the information and click **OK**. To skip the page, click **Cancel**.
5. If the password expired and you are prompted to enter a new password, type `secret` for the old and new passwords.

6. Log out as the user and repeat these steps for the next user in the table.

   Each user has a different interface view, depending on their group ACIs.

Assigning a service owner to the IBM Security Identity Manager service

This scenario assigns a service owner to the Security Identity Manager service.

Before you begin

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

First, log in to the Security Identity Manager administrative console as `itim manager`.

About this task

James Owner is a systems administrator, who maintains several systems and department applications. James is a service owner of the Security Identity Manager system. Service owner responsibilities include creating and modifying provisioning policies and workflows for services. Those tasks are defined in later service owner scenarios.

To assign James as a service owner, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Manage Services**.
3. On the **Select a Service** page, complete these steps:
   a. In the **Services** table, type `ITIM Service` in the **Search information** field and click **Search**.
   b. Select the ITIM Service and click **Change**.
4. On the **Change Service** page in the **Owner** field, click **Search**.
5. On the **Select People** page, type `James Owner` and click **Search**.
6. Select the radio button next to James Owner and click **OK**.
7. On the Success page, click **Close**.

Configuration of a manual service

In this scenario, you configure a manual service that handles requests to use a ledger service. The service requires an employee to do a manual activity, and indicates its success.

A manual service is useful to handle custom applications with few users or an application that does not have an adapter. In this case, the cost of development of a custom adapter might not justify the cost savings gained from automation. Manual service advantages include a self-service user interface, workflow approvals, and audit trail for corporate compliance, avoiding the cost of developing a custom adapter.

Tasks in this scenario include creating a service type for the manual service and customizing account and service forms. You then create the service, set its default values, and assign a service owner.

Creating a manual service type

The first step in this scenario creates a manual service type by adding a schema class to LDAP.

Before you begin

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

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

The insurance company provides reinsurance for a few small satellite companies. Employees in a small accounting department at the insurance company use an old ledger system that interfaces with a department in one of these satellite companies. This ledger system handles the general ledger and also functions as a financial record keeping and reporting system.

The old ledger system is slated for removal over the next two years. Management believes that the expense of developing a custom adapter to interface with Security Identity Manager is too great. However, management wants to track people who use the ledger system to facilitate auditing and regulatory compliance initiatives. For this purpose, the system administrator is tasked with creating a manual service.

This step creates a manual service type called LedgerSystem. The LedgerSystem service type initially has these account attributes:

Table 3. Attributes in the example service type

Attribute	Required
employeeNumber	Yes.
Password	Remove this attribute, which is not needed for a ledger system.
User ID	You cannot change this attribute. Accept the default.
employeeName	Yes.

To create the service type by specifying a new LDAP schema class that has a employeeName attribute for the manual service, complete these steps:

Procedure
1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Configure System** > **Manage Service Types**.
3. On the Manage Service Types page, click **Create**.
4. On the General notebook tab, complete these fields:

Service Type Name
Type `LedgerAccount`. This value becomes the service type name. Do not include spaces in the name. This name is a new LDAP class that you create during this scenario. Avoid specifying an identical value in the **LDAP class** and the **Service Type Name** fields.

Description
This field is read-only.

Service Provider
Select **Manual**.

5. Click the Service notebook tab and complete this field:

LDAP class
Type `LedgerService`. Do not include spaces in the name. This entry is a new LDAP class that you create during this scenario. Avoid specifying an identical value in the **LDAP class** and the **Service Type Name** fields.

6. Click the Account notebook tab and complete these steps:

   a. In the **LDAP class** field, type `LedgerProfile`. Do not include spaces in the name.

   b. In the **Attributes** table, click **Add**, type each of these attributes in the **Attribute name** field and then click **OK** to add each attribute:

      • `employeeName`

      For employeeName, select **Required** and **Directory String**.

      • `employeeNumber`

      For employeeNumber, select **Required** and **Directory String**.

   c. In the **Attributes** table, check the **Password** attribute and click **Remove**.

7. Click **OK** to create the service type.

8. On the Success page, click **Close**. You might see the following warning message: `CTGIMU817W The attributes were not updated due to the following LDAP warnings: * CTGIMO111E Fail to add or update schema for attribute [employeeNumber]. Reason: [LDAP: error code 80 - Other].`

9. Click **Close**.

10. On the navigation tree, click **Configure System** > **Manage Service Types**. Validate that a LedgerAccount item exists in the **Service Type** column.

Customizing an account form

The next step in this scenario is to format a request page that users can access later. You need to specify the contents of the page.

Before you begin

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

About this task

Customizing the account form provides an opportunity to make the user interface more logical to the users who request accounts. The default account form might contain additional fields that display information that users do not need, such as service information. As part of customizing the user interface for a manual service, this task removes unnecessary fields.

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

To customize the account form, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. On the navigation tree, click **Configure System** > **Design Forms** to launch the Form Designer applet, which requires an interval of time to load.

   The first time that the Form Designer runs, the applet installs the Java™ Runtime Environment on your computer. When the Java Runtime Environment is installed, accept the defaults. Click **Finish** when the installation wizard completes.
3. On the Design Forms page, double-click the **Account** folder to load the profile tree. Loading profiles requires an interval of time.
4. In the list of profiles, double-click **LedgerAccountAccountProfile**. Loading profile attributes requires an interval of time.

   The **LedgerAccount** account form contains the attributes from the service type:

Table 4. Attributes in the example Account form

Attribute name in Account form	Keep or delete?
$erobjecttype	Delete
$eruri	Delete
$employeenumber	Keep
$eruid	Keep
$ersponsor	Delete
$employeename	Keep

5. In the account template on the LedgerAccountAccountProfile page, complete these steps to modify the list of attributes:

   a. Delete the unnecessary attributes from the table. Right-click the attribute and then select **Delete Attribute** in the list.

   b. Change the format of the field names to make them more understandable for the user:

   - $employeenumber

     Select the *$employeenumber* attribute. In the Properties section of the page, click the **Format** tab. In the **Label** field, replace the value *$employeenumber* by typing `Employee number for Ledger`.

   - $employeename

     Select the *$employeename* attribute. In the Properties section of the page, click the **Format** tab. In the **Label** field, replace the value *$employeename* by typing `Employee name`.

   Alternatively, if translation is important, do not change the labels of the field names in the Form Designer. Instead, specify a value for the *employeename* attribute in the `CustomLabels.properties` file. For example, specify this string value for the *employeename* attribute:

   ```
   # LedgerAccount attributes
   employeename=Employee name
   ```

The `Customlabels.properties` file is located in the `data` directory in the installation directory. For example:

- Windows

    drive:\IBM\isim\data\CustomLabels.properties

- UNIX, Linux, and AIX

    /opt/IBM/isim/data/CustomLabels.properties

To display the value that you specified in the `CustomLabels.properties` file, restart Security Identity Manager.

Other languages can be enabled by adding the corresponding entries to `CustomLabels_es.properties` (Spanish), `CustomLabels_jp.properties` (Japanese). If a label is not found for a language that the user prefers, then the value in `CustomLabels.properties` is used.

   c. Reorder the attributes for ease of use by selecting an attribute and clicking the up arrow icon in the Form Designer menu bar. If the attribute is not at the top of the list, position the *$eruid* attribute uppermost, followed by the *$employeename* and *$employeenumber* attributes. Alternatively, you can right-click an attribute and click **Move Up Attribute** in the menu.

   d. On the Form Designer task bar, click **Form** > **Save Form Template**.

   e. Click **OK** on the success message page.

6. Double-click the **Service** folder to open the Service template on the LedgerAccount page.

7. Double-click **LedgerAccount**.

   The Service form contains these attributes:

Table 5. Attributes in the example Service form

Attribute name in Service form	Keep or delete?
$eruid	Delete
$erservicessomapping	Delete
$owner	Keep. The attribute tells the administrator who the service owner is.
$ertag	Delete
$erprerequisite	Delete
$eruri	Delete
$erpassword	Delete
$description	Keep
$erservicename	Keep

   a. Delete the unnecessary attributes. Right-click the attribute and then select **Delete Attribute** in the list.

   b. Change the control type of the *$owner* attribute to a search capability for a specific user as the service owner.

      1) Select the Service Owner attribute. Run the mouse across the icons in the Form Designer menu bar until you locate Search Control (a magnifying glass icon). Click the Search Control icon.

      2) In the Search Control Editor page, select **Person** as the category and click **OK**. The *$owner* attribute changes to indicate that it references the Search Control control type. This control type causes a list of users to be displayed when the administrator clicks the **Search** button next to this field.

c. Order the attributes for ease of use by selecting an attribute and clicking the up arrow icon in the menu bar.

Position the *$erservicename* attribute uppermost, followed by the *$description* and *$owner* attributes. Alternatively, you can right-click an attribute and click **Move Up Attribute** in the menu. This arrangement is the vertical order of field labels in the page when you later create a service for this service type.

8. On the Form Designer task bar, click **Form** > **Save Form Template**.

9. Click **OK** on the success message page.

10. Click **Close** to close the Form Designer applet.

Creating an access control item for a manual service

The next step in this scenario is to create an access control item for the manual service. For example, the access control item grants permission to users to write a value such as an employee number or employee name when they request a ledger account.

Before you begin

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

About this task

Creating an access control item gives you the ability to securely make this service available to users other than administrators.

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

To create an access control item for the manual service, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.

2. From the navigation tree, click **Set System Security** > **Manage Access Control Items**.

3. On the Manage Access Control Items page, click **Create**.

4. On the General wizard page, complete these fields and then click **Next**:

   Name Type `Ledger_ACI`.

   Protection category
   Select **Account**.

   Object class
   Select **LedgerProfile**.

5. On the Operations wizard page, click **Next** to skip to the next tab.

6. On the Permissions wizard page, grant Read and Write permission for the employeeName and employeeNumber attributes. Then, click **Next**.

7. On the Membership page, check the **Account owner** check box to specify that the access control item applies to only those accounts that are owned by the user. Do not select other check boxes.

8. Click **Finish** to save the access control item.

9. On the Success page, click **Close**.
10. On the Manage Service Types page, click **Close**.

Creating a manual service

The next step in this scenario is to create a manual service and specify its default values.

Before you begin

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

About this task

In a previous step, the administrator created a type of manual service. This step creates an instance of that type of service, and defines James Owner as the service owner.

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

To create a manual service, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Manage Services**.
3. On the Select a Service page in the **Services** table, click **Create**.
4. On the Select the Type of Service page, select **LedgerAccount** as the service type. Then, click **Next**. The list of service types might span several pages.
5. On the General Information wizard page, the field labels occur in the sequence that you previously specified on the Service template. Complete these fields and then click **Next**:

   Service name

   Type LedgerAccount.

   Description

   Type Reinsurance Satellite Ledger System.

   Owner

   Click **Search**. On the Select Users page, click **Search** again. In the **Users** table, select **James Owner** as the owner and then click **OK**.

6. On the Participants page in the **Participant type** field, select **Service owner**. In the **Escalation participant type** field, select **Administrator**.
7. Accept the default for escalation interval and click **Next**.

   If the service owner, James Owner, does not respond within the escalation interval, the Security Identity Manager administrator receives the request in an activities list. If you select a group, an escalated request goes to request to all members of that group.

8. On the Messages page, click **Next**.
9. On the Configure Policy page, click **Next**.
10. On the Reconciliation page, click **Finish**.

A reconciliation file for a manual service might serve the purpose of loading additional data that has a narrow scope. For example, data might be a set of matching user IDs and preassigned employee numbers.

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

    Click **Close** again if you need to close any remaining pages for this task.

Creating default values to reduce user effort

The next step is to set default values to reduce the tasks that users must complete to request an account on the manual service. For example, you might provide a default value for the user's employee number.

Before you begin

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

About this task

There are some account attributes for which a user does not know the value, or the administrator prefers to define a value. Commonly, a service owner is tasked with doing this step.

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

To specify default values, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. In the navigation tree, click **Manage Services**.
3. On the Select a Service page, in the **Service Type** field, select **LedgerAccount** from the list and then click **Search**.
4. In the **Services** table, click the icon (▸) next to the **LedgerAccount** service and then select **Account Defaults**.
5. On the Select an Account Attribute page, click **Add**.
6. On the Select an Attribute to Default page, select **Employee number** and click **Add (Basic)**.
7. On the Employee number for ledger page, complete these fields:

    Prepend text
    Enter a value that represents a common, first element in all employee numbers. For example, enter the value 1A if all employee numbers begin with 1A.

    User attribute
    Click **Search**. Select the **Employee number** attribute and click **OK**.

    Append text
    Leave this field blank.

8. Click **OK** to return to the Select an Account Attribute page.

    Validate that the prefix for **{Employee Number}** is now in the **Template value** field.

9. Click **OK** to save the account defaults.

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

    Click **Close** again if you need to close any remaining pages for this task.

Access definition on a shared folder

This scenario describes defining an access on a shared folder in IBM Security Identity Manager.

Most employees who work in the same department share information. Often this shared information is stored in a folder so that employees can alternately read, write, and modify information. For easy access to this folder and to create an audit trail to meet compliance criteria, you can define an access on the shared folder.

Access definitions are not limited to shared folders. You can define access on other managed resources, such as email groups and applications.

Installing a Windows local adapter

The first step is to install a Windows local adapter.

Before you begin

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

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

In this example, the administrator installs a Windows local adapter. The Windows local service is later used to define an access to a shared folder.

To run the Windows local adapter installer, complete these steps:

Procedure
1. Open the compressed adapter file.
2. Open the PDF file that contains the installation and configuration guide.
3. Install and configure the Winlocal adapter, following the steps in the installation and configuration guide.

Importing a Windows local adapter profile

The next step is to import the Windows local adapter profile into IBM Security Identity Manager.

Before you begin

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

About this task

After the adapter is installed, the administrator must import the Windows local adapter profile into Security Identity Manager.

To import the Windows local adapter profile, complete these steps:

Procedure

1. Open and extract the compressed adapter file.
2. Place the JAR file that contains the adapter profile in a temporary directory on the computer that is runningSecurity Identity Manager. On clusters, place the JAR file on the computer that hosts the network deployment manager.
3. As administrator, open the Security Identity Manager user interface.
4. Click **Configure System** > **Manage Service Types**.
5. On the Manage Service Types page, click **Import**.
6. On the **Service Definition File** field, click **Browse**. Then, locate the JAR file that contains the Winlocal adapter profile.
7. When the **Service Definition File** field contains the adapter profile file name, click **OK**.
8. On the Success page, click **Close**.

What to do next

Importing an adapter profile is an asynchronous process that might require an interval of time to complete.

Creating a Windows local service

The next step is to create a Windows local service

Before you begin

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

First, log in to the IBM Security Identity Manager administrative console as `itim manager`.

About this task

After the Security Identity Manager administrator imports the profile, a Windows local service needs to be created in Security Identity Manager. In this case, the service in Security Identity Manager represents a user repository in Windows.

To create a Windows local service, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Manage Services**.
3. On the Select a Service page, click **Create**.
4. Click the radio button next to the **Windows Local Account Profile** service type and click **Next**.

5. On the Select the Type of Service page, complete these steps:
   a. In the **Service name** field, type `Windows Local Service`.
   b. In the **URL** field, specify the location and port number of the Windows Local Account Adapter. For example, `http://localhost:45580`
   c. In the **User ID** field, type the User ID of the Windows local service, which is `agent` by default.
   d. In the **Password** field, type the password of the Windows local service, which is `agent` by default.
   e. In the **Owner** field, click **Search**. On the Select Users page, click **Search** again. In the **Users** table, select **James Owner** as the owner and click **OK**.
   f. Click **Test Connection** to confirm you can connect to the service.
   g. Click **Finish**.
6. On the Success page, click **Close**.
7. On the Select a Service page, click **Close**.

Reconciling the Windows local service and loading users and groups into IBM Security Identity Manager

The next step is to reconcile the Windows local service, which adds Windows groups to the system.

Before you begin

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

First, log in to the Security Identity Manager administrative console as `itim manager`.

About this task

Reconciling the Windows local service copies user and group data from Windows and runs policies. When Windows administrators (service owners) create a shared folder, they can set security on the shared folder to a specific Windows group. Only that group can access the folder. Populating groups into the Security Identity Manager system is necessary to define an access to the shared folder.

To reconcile the Windows local service, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Manage Services**.
3. On the Select a Service page, complete these steps:
   a. In the **Search information** field, type `Windows local` and click **Search**.
   b. In the **Services** table, click the icon (▶) next to **Windows local** and click **Reconcile Now**.
   c. On the Select Query page, select **None** and click **Submit**.
4. On the Success page, click **Close**.

   Note: The reconciliation can take a few minutes to complete.

Defining an access entitlement in IBM Security Identity Manager

The next step is to reconcile the Windows local service and define an access entitlement for a shared folder on the Windows system.

Before you begin

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

This task creates an access entitlement for a shared folder named **Presentations** on the Windows system. In order for this task to work, the service owner or administrator must:

- Create in Windows a folder named **Presentations** and a group `Presenters`.
- Make access to that folder available to the `Presenters` group.
- Run a reconciliation to load groups into the Security Identity Manager system.

First, log in to the Security Identity Manager administrative console as `itim manager`.

About this task

A group of accountants needs to manage files for quarterly presentations. Each accountant is responsible for certain files in the presentation; some files overlap responsibilities. To maintain up-to-date records and secure this information, the accountants maintain a shared folder. Turnover in the accounting department makes it time consuming to regularly assign permissions and track users who require continued access to the shared folders. Security Identity Manager is used to facilitate this process.

To define an access entitlement to a shared folder on the Windows system, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Manage Services**.
3. On the Select a Service page, complete these steps:
    a. In the **Search information** field, type `Windows local` and click **Search**.
    b. In the **Services** table, click the icon (▸) next to **Windows local** and click **Manage Groups**.
4. On the Manage Groups page, type `Presenters` and click **Search**. The `Presenters` group is displayed.
5. Select the group and click **Change**. The Change Group page is displayed.
6. On the General Information page:
    a. Click the **Access Information** tab to see the Access Information page
    b. Select the **Define an Access** check box to activate the access description fields.
    c. Click **Enable Common Access**.
    d. In the **Access name** field, type `Access to Presentations folder`.
    e. In the **Access type** field, select **Shared Folder**.

f. In the **Description** field, type `Shared Presentations Folder`.

a. Supply any other optional information you want to specify.

b. Click **OK** to submit.

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

Data synchronization for reports

This scenario demonstrates how to synchronize data for reports in IBM Security Identity Manager.

Reports depend on some data that must be synchronized from the LDAP directory to the relational database. Without synchronization, the reports contain no data. Managers and auditors who rely on reports for regulatory compliance have no information with which to work. Set up a synchronization schedule to keep the data in the relational database up to date.

Synchronizing data for reports in IBM Security Identity Manager

This scenario synchronizes data for audit-related reporting in Security Identity Manager.

Before you begin

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

You must first be logged in to the Security Identity Manager administrative console as `itim manager`.

About this task

To synchronize report data, complete these steps:

Procedure

1. Log in to the administrative console as an administrator.
2. From the navigation tree, click **Reports** > **Data Synchronization**.
3. On the Data Synchronization page, click **Run Synchronization Now**.
4. On the Confirm page, click **Run Synchronization Now**.

   Note: Data synchronization can take a few minutes to complete.

Chapter 3. Service owner scenarios

These scenarios demonstrate some of the advanced tasks that a service owner would do to set up IBM Security Identity Manager for a production environment.

Service owners are responsible for maintaining and controlling access to IT systems. Service owners can be application owners, developers, or system administrators. A service owner can be anyone who has responsibility over a managed resource, which can include manual services. These tasks can help a service owner make service available for others to securely request and manage user accounts across the enterprise. The service owner sets up services with appropriate access rules, approvals, and audit trail.

Configuration of an approval workflow for a manual service

In this scenario, a service owner configures an approval workflow for a manual service, which requires a manager to approve a new service request.

In the past, approvals were done by sending email messages to managers or sending paper forms. With IBM Security Identity Manager, a service owner can automate the approval process online.

Tasks in this scenario include creating a workflow for the manual service and adding a provisioning policy for the workflow.

Creating an account request workflow for a manual service

The first step in this scenario is to create a workflow that is used whenever an account is requested for the service that you created.

Before you begin

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

In the previous administrator scenario, the administrator created a manual service named LedgerAccount. In this scenario, the service owner of this manual service creates an account request workflow for that service.

About this task

To design an account request workflow, complete these steps:

Procedure

1. Log in to the administrative console as service owner jowner.
2. From the navigation tree, select **Design Workflow** > **Manage Account Request Workflows**.
3. On the Manage Account Request Workflows page, in the **Account Request Workflows** table, click **Create**.
4. On the General notebook page, type the following information for your workflow:

Name Type Ledger service approval.

Description
>   Type Approval for the LedgerAccount service.

5. From the **Service type** dropdown list on the General notebook page, select **LedgerAccount**.
6. Click the **Activities** tab. On the Activities page, complete these steps:
    a. In the **Select method for defining activities** field, select **Simple**. If you want to create a different sequence of activities for approval, there is an advanced design.
    b. From the **Simple Activities Definition** table, select **Create an approval activity** and then click **Go**.
7. On the Approval Activity page, specify the following information and click **OK**:

    Activity name
    >   Type Manager Approval for ledger accounts.

    Approver type
    >   Select **Manager**.

    Escalation time in days
    >   Type 10. The request escalates to the specified escalation participant when this interval of time expires.

    Escalation participant type
    >   Select **Administrator**.

8. On the Activities notebook page, click **OK**.
9. On the Success page, click **Close**.

Creating a provisioning policy for a manual service

The next step in this scenario is to create a provisioning policy for the workflow that is used to provision an account for the manual service.

Before you begin

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

In the previous scenario, the service owner designed a workflow approval for a manual ledger service. The accounting department that uses the ledger service can request approval to use the ledger service. In this scenario, the service owner creates a provisioning policy for that workflow. This service does not create any automation to log in and use the ledger system; that process is done manually by the service owner.

About this task

Provisioning policies are a central place to manage how services are made available to users. There are options for automation, manual requests, and ongoing monitoring of compliance of accounts.

To create a provisioning policy, complete these steps:

Procedure

1. Log in to the administrative console as service owner jowner.

2. From the navigation tree, select **Manage Policies** > **Manage Provisioning Policies**.
3. On the Manage Provisioning Policies page, click **Create**.
4. On the General notebook page, type the following information for your policy:

   Policy name
   > Type `Ledger service provisioning policy`.

   Description
   > Type `Provisioning policy for the Ledger service`.

   Leave the other default information as provided.
5. Click the **Entitlements** tab. On theEntitlement notebook page, click **Create**.
6. On the Account Entitlement page, complete these steps and click **OK**:
   a. In the **Provisioning options** field, select **Manual**.
   b. In the **Target type** field, select **Specific Service**.
   c. In the **Service type** field, click **Search**, run a service and select **LedgerAccount** in the search results.
   d. In the **Workflow** field, click **Browse**, select **LedgerAccount** in the **Search by** field, click **Search**, select **Ledger service approval** and click **OK**.
7. On the Entitlements notebook page, click **Submit**.
8. On the Schedule page, accept the default settings and click **Submit**.
9. On the Success page, click **Close**.

Configuration of an approval workflow for the Windows local service

In this scenario, the service owner configures an approval workflow for the Windows local service, which requires a manager to approve a new service request.

Tasks in this scenario include creating a workflow for the Windows local service and adding a provisioning policy for the workflow.

Creating an account request workflow for the Windows local service

The first step in this scenario is to create a workflow that is used whenever an account is requested for the Windows local service.

Before you begin

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

In the previous administrator scenario, the IBM Security Identity Manager administrator assigned a service owner to the Windows local service. In this scenario, the service owner creates an account request workflow for that service.

About this task

To design an account request workflow, complete these steps:

Procedure

1. Log in to the administrative console as service owner `jowner`.

2. From the navigation tree, select **Design Workflow** > **Manage Account Request Workflows**.

3. On the Manage Account Request Workflows page in the **Account Request Workflows** table, click **Create**.

4. On the General notebook page, type the following information for your workflow:

   Name   Type `Windows local service approval`.

   Description
   > Type `Approval for the Windows local service`.

5. From the **Service type** list on the General notebook page, select **Windows Local Account Profile**.

6. Click the **Activities** tab. On the Activities page, complete these steps:

   a. In the **Select method for defining activities** field, select **Simple**. If you want to create a different sequence of activities for approval, there is an advanced design.

   b. From the **Simple Activities Definition** table, select **Create an approval activity**and click **Go**.

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

   Activity name
   > Type `Manager Approval for Windows local accounts`.

   Approver type
   > Select **Manager**.

   Escalation time in days
   > Type 10. The request escalates to the specified escalation participant when this interval of time expires.

   Escalation participant type
   > Select **Administrator**.

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

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

Configuration of an approval workflow for an access entitlement

In this scenario, the service owner configures an approval workflow for an access entitlement. The entitlement (a shared folder) is defined for a service and requires manager approval.

A service owner can add an approval workflow for an access entitlement in addition to, or instead of, the user account as a whole. This entitlement can be especially useful if the resources that are being accessed by user groups have owners that need to participate in approval workflows. Optionally, an additional level of approval that is supported applies to group assignments for accounts. This level can be implemented by a workflow for access entitlements.

Tasks in this scenario include defining an access entitlement, creating an access approval workflow, and creating a provisioning policy for the workflow.

Creating an access request workflow

The first step in this scenario is to create a workflow that is used whenever access is requested.

Before you begin

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

About this task

In the previous administrator scenario, the IBM Security Identity Manager administrator created an access entitlement. In this scenario, the service owner creates a request workflow for that access.

After this workflow is created, an accountant can request access to the shared folder. For instance, if Judith User wants to access this shared folder, 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 period specified, the service owner must respond.

To design an access request workflow, complete these steps:

Procedure

1. Log in to the administrative console as service owner `jowner`.
2. From the navigation tree, select **Design Workflow** > **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   Type `Windows shared folder access workflow`.

   Description
   Type `Approval for the Presenters group`.
5. From the **Service type** list on the General notebook page, select **All**.
6. Click the **Activities** tab. On the Activities page, complete these steps:

   a. In the **Select method for defining activities** field, select **Simple**.

   b. From the **Simple Activities Definition** table, select **Create an approval activity**and click **Go**.
7. On the Approval Activity page, specify the following information and click **OK**:

   Activity name
   Type `Manager Approval for Windows shared folder access`.

   Approver type
   Select **Manager**.

   Escalation time in days
   Type 10. The request escalates to the specified escalation participant when this interval of time expires.

   Escalation participant type
   Select **Service Owner**.
8. On the Activities notebook page, click **OK** again.
9. On the Success page, click **Close**.

Chapter 4. Non-administrative user scenarios

These scenarios demonstrate some of the simple tasks that a non-administrative user would do in IBM Security Identity Manager.

Judith User is an accounting team lead reporting to Chuck Manager. Daily accounting tasks require an account on a Windows system and access to a shared folder to update presentation material.

Access request to resources

These scenarios demonstrate how to request accounts and access entitlements in IBM Security Identity Manager.

Requesting a Windows local service account

The first step in this scenario is to request a Windows local service account.

Before you begin

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

In the previous service owner scenario, the service owner designed an approval process for the Windows local service. In this scenario, Judith User requests approval for an account on that service.

About this task

This scenario is designed to show how the account approval process works. Across organizations, resources can vary to which a user typically requests an account. If you do not have access to a Windows service, this approval process can work with the ITIM Service as well.

To request a Windows local service account, complete these steps:

Procedure
1. Log in to the self-service console as user `juser`.
2. On the Home page, click **Request Account**.
3. Click the link labeled **Windows Local Service**.
4. On the Account Information page, verify your user ID and click **Next**.
5. Review the information and click **Request Account**.
6. Click the **Home** breadcrumb at the top to return to the Home page.

Requesting access to a shared folder

The next step in this scenario is to request access to a shared folder in Windows.

Before you begin

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

In a previous scenario, the service owner designed an approval process for a shared folder. In this scenario, Judith User requests approval for access to that shared folder.

About this task

As accounting team lead, Judith User needs to access a shared folder named Presentations. Judith shares this folder with colleagues in the accounting department. The colleagues put together slides and other material for Chuck Manager to present in quarterly meetings to upper management.

To request access to a shared folder, complete these steps:

Procedure

1. Log in to the self-service console as user `juser`.
2. On the Home page, click **Request Access**.
3. Click the link labeled **Access to Presentations folder**.
4. On the Request Access page, review the information and click **Request Access**.
5. Click the **Home** breadcrumb at the top to return to the Home page.

Checking out a credential or credential pool

Use this procedure to use privileges not associated with your normal account.

Before you begin

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

About this task

Credentials to obtain shared access are used by multiple users based on roles. They enable users to temporarily access needed applications. The checkout process places an exclusive lock on the credential. No other user can use the same credential concurrently.

Procedure

1. Log in to the self-service console.
2. On the Home page, click **Check out Credential**.

   The Check out Credential page lists the credentials that you are authorized to access.

   - If you see the credential you want to access, continue to step 3 on page 35.
   - If you do not see the credential you want, you can search for additional credentials:
   a. In the Search for Credential section of the page, click **Search**. The Search for Shared Credential page is displayed.

b. Enter the name of the credential or credential pool that you want to access or specify additional search criteria. Click **Search**.

You can filter based on Service Type, Account Type, or Organizational Unit. You can specify that the search includes credentials for which you do not have authorization. See the online help for more details on the filters.

Optionally, you can click **Browse** to search for organizational units. If you click **Browse**, the Search for Organizational Unit page is displayed. Specify search filters and click **Search**.

The search returns a Search Results table that contains a list of credentials.

3. Click the credential that you want to check out.

- If the Checkout Information page is displayed, you are authorized to access the credential. Continue with step 4.

- If the Select Role page is displayed, you are *not* authorized to access the credential. You must request a role to access the credential or credential pool. Complete the following steps:

a. Select a role that has access authority for the selected shared credential or credential pool.

The table lists the roles that have access authority. You must obtain membership in one of the roles in order to check out the credential or credential pool.

b. Review the list of shared access entitlements for the role that you selected and click **Submit**. A new page describes the request you submitted.

c. A new page describes the request you submitted. Select one of the action links at the bottom of the page:

- Click **View My Requests** to look at the status of your request.

You must wait until your request is completed in order to continue with the check out of the credential or credential pool.

- Click **Check Out Credential** to check out another credential.

- Click the **IBM Security Identity Manager Home** link to return to the home page for the self service console.

d. Return to step 2 on page 34.

4. Review the fields on the Checkout Information page and then complete the checkout.

By default, this page contains only the **Credential checkout expiration time** field and the **Justification** field, but your administrator might specify additional fields.

a. The **Credential checkout expiration time** field contains the date and time when your access to the credential expires. The administrator specifies the default maximum allowed lifetime for each checked-out credential. You can modify the expiration time to shorten the lifetime of the checked-out credential; however, you cannot extend the lifetime.

b. In the **Justification** field, explain the reason you need access to the credential. By default, this field is optional.

c. Click **Check out**. The Checkout Confirmation page is displayed.

What to do next

Use the user ID and password that you checked out to log on to the application that you want to use.

Viewing the password for a shared credential

Use this procedure to view the password for a shared credential from the credential vault.

Before you begin

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

About this task

You can view the password for shared credentials that you are authorized to access. Some credentials require that you check them out from the credential vault before you can view the password. If you do not have authority to access a credential, you can request it.

Your administrator can choose not to register passwords for some credentials. Your administrator can also specify that some registered passwords are not viewable through the self service console. For these credentials, you must contact the system administrator in order to view the password.

Procedure

1. Log in to the self-service console.
2. On the Home page, click **View Password**.

   The View Password page displays a list of the credentials that you checked out.
   - If the list contains the credential you want to access, click the credential name link. The View Password Details page displays the password value in the **Password:** row. If the password is not displayed because it is not registered or not viewable, contact your system administrator.
   - If the list does *not* contain the credential you want to access, you can search for additional credentials.
3. Search for additional credentials:
   a. In the Search for Credential section of the page, click **Search**. The Search for Shared Credential page is displayed.
   b. Enter the name of the credential or credential pool that you want to access or specify additional search criteria. Click **Search**.

      Note: You can specify search criteria based on Service Type, Account Type, or Organizational Unit. You can also specify whether the search results include credentials that you do not have authority to access. See the online help for more details on how to use the search criteria.
4. The search returns a Search Results table that contains a list of credentials. Click the credential for which you want to view the password. Complete one of the following steps, depending on which panel is displayed:
   - If the Checkout Information panel is displayed, continue with step 5 on page 37.
   - If the Select Role panel is displayed, continue with step 6 on page 37.
   - If the View Password Details panel is displayed, continue with step 7 on page 37.

5. The Checkout Information panel is displayed when the shared credential requires check out to view the password and you have authority to complete the checkout. Supply the requested information in the Checkout Information panel and click **Check Out**.

   The Checkout Confirmation page displays. You can view the password in the Password field.

   If the Checkout Confirmation page does *not* display, review the error or information message and contact your system administrator.

   Note: Credential checkout can be denied for reasons unrelated to viewing a password. For example, the credential pool might not have any credentials available for checkout at the current time.

6. The Select Role panel is displayed when you do *not* have authority to access the credential or credential pool. To obtain authority complete the following steps:

   a. Select a role that has access authority for the selected shared credential.

      The table lists the roles that have access authority. You must obtain membership in one of the roles in order to view the password for the credential.

   b. The Request Role panel is displayed. Review the list of shared access entitlements for the role that you selected. If these entitlements are correct for the task you want to accomplish, click **Submit**.

   c. A success page describes the request you submitted. Select one of the action links at the bottom of the page:

      - Click **View My Requests** to look at the status of your request.

        In order to view the password, you must wait until the request completes. When your request completes, restart the View Password task.

      - Click **View Password** to view another password.

      - Click the **IBM Security Identity Manger Home** link to return to the home page for the self service console.

   d. Return to step 2 on page 36.

7. If the shared credential does *not* require check out and you have authority to access the credential, the View Password Details page displays the password value in the **Password:** row.

   If the password is not displayed, and a message indicates that the password is not registered or not viewable, contact your system administrator.

Chapter 5. Manager scenarios

These scenarios demonstrate some of the simple administrative tasks that a manager would do in IBM Security Identity Manager.

Chuck Manager is a controller who manages a team of accountants. The accountants need access to certain resources, such as shared folders and accounts on services. IBM Security Identity Manager provides the workflow and reporting capabilities for managers to approve requests, do recertification activities, and generate reports for regulatory purposes. These scenarios describe a subset of these activities to demonstrate these capabilities.

Approval of user requests

This scenario describes how to approve different user requests in IBM Security Identity Manager.

In the previous user scenario, the user Judith requested an account and access on the IBM Security Identity Manager service. In this scenario, Chuck Manager approves the request for an account and an access entitlement for the user on that service.

Approving an account request

The first step describes how to approve user account requests in IBM Security Identity Manager.

Before you begin

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

About this task

Judith User recently made a request to Chuck Manager to access an account on a Windows service. Chuck verified that Judith needs this account to do daily tasks and wants to approve the request.

To approve an account request on the Windows local service, complete these steps:

Procedure
1. Log in to the self-service user interface as user `cmanager` with password `secret`. Alternatively, you can log in to the administrative console user interface to do these activities.
2. On the Home page, click **Approve and Review Requests**.
3. Click the link labeled **Manager approval for Windows local accounts**.
4. On the Review Request page, select the **Approve** action and click **OK**. Alternatively, add reviewer comments and click **OK**.
5. Click the **Home** breadcrumb at the top to return to the Home page.

Approving an access request

The next step describes how to approve access requests in IBM Security Identity Manager.

Before you begin

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

About this task

Judith User requests access to a shared folder named Presentations. Chuck Manager requires Judith to access this folder to update presentation material for the quarterly meetings that Chuck has with a manager. Chuck wants to approve this access request.

To approve an access request on a shared folder, complete these steps:

Procedure

1. Log in to the self-service user interface as user `cmanager` with password `secret`. Alternatively, you can log in to the administrative console user interface to do these activities.
2. On the Home page, click **Approve and Review Requests**.
3. Click the link labeled **Manager Approval for Windows shared folder access**.
4. On the Review Request page, select the **Approve** action and click **OK**. Alternatively, add reviewer comments and click **OK**.
5. Click the **Home** breadcrumb at the top to return to the Home page.

Chapter 6. Identity Service Center scenarios

These scenarios demonstrate some of the tasks that a manager or representative can do in the Identity Service Center.

Exporting the CSV file to update the services access data

This scenario describes how to export the comma-separated value (CSV) file and edit the service access data that it contains.

About this task

You can edit the following access data to configure what is displayed in the Identity Service Center: **Service DN**, **Service name**, **Define as Access**, **Access name**, **Access type**, **Access description**, **Icon URL**, **Search terms**, **Additional information**, and **Badges**.

Procedure

1. Log in to the IBM Security Identity Manager console.
2. Go to **Manage Services**.
3. Click **Refresh** to show the list of access data you have.
4. Select the services or access data that you must update.
5. Click **Export Access Data**.

   Note: If there are any processing errors, a message is displayed. Click **Download Export Log File** for details on how to fix the error.
6. Click the **Download Exported Data**.
7. Select **Save File**.
8. Click **OK**.
9. Open the file to edit.
   a. From the **Downloads** dialog box, select the downloaded file.
   b. Select **Open** from the menu.
   c. Open the CSV file in any of the following tools to see the access details:
      - IBM Lotus Notes® Symphony®
      - Microsoft Excel
      - Google Docs
10. Edit the access details.

    You can modify only the access information but not entity information like **Service name**, **Group name**, or **Role name**. If you try to edit them, the updates are not carried over in the Identity Service Center.

What to do next

Go to the Identity Service Center and verify the updates that you made in the access data.

Importing the CSV file to update the services access data

This scenario describes how to import the comma-separated value (CSV) file and edit the service access data that it contains.

About this task

You can edit the following access data to configure what is displayed in the Identity Service Center: **Service DN**, **Service name**, **Define as Access**, **Access name**, **Access type**, **Access description**, **Icon URL**, **Search terms**, **Additional information**, and **Badges**.

Procedure

1. Log in to the IBM Security Identity Manager console.
2. Go to **Manage Services**.
3. Click **Import Access Data**.
4. Click **Browse** to search for the file that you want to import and update.
5. Click **Open**.

   A confirmation message indicates whether the file is uploaded or the import process is complete.

   Note: If there are any processing errors, a message is displayed. Click **Download Import Log File** for details on how to fix the error.
6. Open the file to edit.
   a. From the **Downloads** dialog box, select the downloaded file.
   b. Select **Open** from the menu.
   c. Open the CSV file in any of the following tools to see the access details:
      - IBM Lotus Notes Symphony
      - Microsoft Excel
      - Google Docs
7. Edit the access details.

   You can modify only the access information but not entity information like **Service name**, **Group name**, or **Role name**. If you try to edit them, the updates are not carried over in the Identity Service Center.

   Note: Any other value in the DEFINE_AS_ACCESS field in the CSV file other than TRUE, is considered FALSE.
   If you leave the field blank, or if you entered any random character in the DEFINE_AS_ACCESS field, the entry or blank space is considered as FALSE.

What to do next

Go to the Identity Service Center and verify that the updates are displayed.

Launching the IBM Security Identity Governance home page from the Service Center

You can used IBM Security Identity Manager to create a task to launch the Security Identity Governance application home page from the Identity Service Center.

Before you begin

You must have administrative user permissions to perform this task.

About this task

To launch the Security Identity Governance home page from the Identity Service Center you must create a custom task and configure a view.

Procedure

1. Obtain the URL for the Security Identity Governance home page.
2. Log on to the Security Identity Manager Console.
3. Create a custom task
   a. Click **Set System Security** > **Manage Views**.
   b. Click **Manage Custom Tasks**.
   c. Click **Create**.
   d. Fill out the Create Custom Task form. Use the values provided in this table.

Table 6. Values needed for this custom task

Field	Value
Identifier prefix	Preset as **CUSTOM_**
Identifier suffix	`SIG`
Description	`Launch Identity Governance Application.`
URL	The URL for the Identity Governance application that you obtained in step 1.
Icon	`http://`*ip_address*`:`*port*`/itim/ui/custom/ui/images/Home-IdentityGovernce.png` where **ip_address** Is the address of the IBM Security Identity Manager server. **port** Is the HTTP or HTTPS port for the Security Identity Manager Web application.
Header category	`CUSTOM_SIG`
Console	Preset as **Service Center**.

   Ensure that you select the check boxes for **Show on home page** and **Start task in new window**.
   e. Click **OK**.
4. Enable the new custom task in the Security Identity Manager views.
   a. Click **Click Set System Security** > **Manage Views**.
   b. Click Search
   c. Click the view you want to modify.
   d. Click **Configure View**.
   e. Scroll to Service Center and select the check box for **Govern Access**.
   f. Click **OK**.
5. Log out of the Administrative console.
6. Log on to the Identity Service Center to verify that the task is displayed on the home page.

What to do next

Launch the Security Identity Governance home page.

Logging in and out from the Identity Service Center

This scenario describes how to log in and out from the Identity Service Center. Use a web browser to access the login page. You can establish either a secure (HTTPS) or unsecure (HTTP) connection to the Identity Service Center.

Before you begin

Use the Identity Service Center Login page URL that is provided by your site administrator. The URL contains settings that were used when the Identity Service Center was installed and configured. For example, the URL might be:

- `http://hostname:port/itim/ui/`
- `https://hostname:port/itim/ui/`

This URL is made up of:

- The name of the host system `http://hostname` that runs the Identity Service Center. *hostname* is the name or IP address of the system where your product is installed.
- The *port* number of the Identity Service Center. For example, `9080`.
- The context for the Identity Service Center. This part is always the same: `/itim/ui/`

Ensure that the correct URL is established.

Note: The default setting for Microsoft Internet Explorer, version 10 is **Browser mode: IE10**. Make sure that you use the default setting, otherwise all the login elements in the page might not display properly. For more information, see *Identity Service Center login orientation error in Internet Explorer 10.0* in *IBM Security Identity Manager Troubleshooting Guide*.

Follow these steps to log in or log out the Identity Service Center.

Procedure

1. Enter the Identity Service Center URL in your web browser. For example, enter:
   `http://your_co.com:9080/itim/ui/`
2. Enter your user name in the **User ID** field.
3. Enter your password.
4. Click **Log in** to open the Identity Service Center.

   Note: Login errors can occur for reasons, which include:
   - Either the user name or password is not specified. Both of these fields are mandatory.
   - The specified user name and password do not pass the authentication process.
   - A network communication error occurred.

   When the login process fails, an error message is displayed. Log in to the Identity Service Center again to correct any login errors.
5. Click **Log Out** when you are done with your tasks.

Note: For left-to-right text orientation, for example, English or French, the **Log Out** link is on the upper right of the screen. For right-to-left text orientation, for example, Hebrew or Arabic, the **Log Out** link is on the upper left of the screen.

Results

When you log out the Identity Service Center, you are redirected to the Login page. For security reasons, log out after you complete your session.

Requesting access for yourself with the Identity Service Center

This scenario describes how to use the Identity Service Center Request Access wizard to provide you access, such as role membership, accounts, services, and groups. The wizard provides a unified catalog of access that you can use.

Before you begin

Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access to this task.

The system configuration, such as access catalog information and provisioning policies, affects the users and accesses that can be selected in this flow.

Follow your organization process for any operations or permissions to make sure that your request is valid.

About this task

Use the Request Access wizard to request one or more accesses for yourself from the unified catalog of accesses. The wizard supports batch requests by building up a list of items to request before you go to the next step. For example, you move into a new role, and you require access to multiple systems or applications.

Procedure

1. Log on to the Identity Service Center.
2. From the Identity Service Center Home page, click **Request Access** to display the Select accesses page. If your view is for self and others, the Select user page is displayed. Click **Select me** from the **Quick Select** menu.
3. On the Select accesses page, select one or more accesses.

   Note: A message is displayed if you exceed the maximum limit that is set for selecting the access. If no maximum limit is set, the default access selection limit is 25.

   The request summary area displays an updated summary about your access selections. Any errors, warnings, or information messages about the access selections are also displayed there. Click the area to open and view the **Request summary** details.

   Request access for
   > Displays your name.

   Request access to
   > Displays the accesses that you selected.

   If you want to start with your request again, then click **Cancel my request**.
4. Click **Next** to open the Provide required information page.

5. Provide a brief description or justification about your business requirement for the access items that you are selecting.
6. Depending on the configuration, click **Provide account information**, if it is displayed, to open the Account information page. Specify the additional information that is necessary for your request, such as personal information, or necessary resource-specific information.

   Note: For non-compliant values or validation errors in any Identity Service Center console fields, click outside the field or tab to view or display the updated hover or hint text.

   After the account information is entered, click **Continue request** to return to the Provide required information page.
7. If you have existing accounts on the resource, specify the account or multiple accounts to which the access is applied.
8. Click **Submit**. A message is displayed to indicate a successful submission or any submission errors.

What to do next

Depending on your view setting, you can view the confirmation and status of your submitted request in the View requests page. To do so, go to **Home** > **View Requests**.

Request more accesses for the selected user, or specify new accesses for another user.

Requesting access for a user in the Identity Service Center

This scenario describes how to use the Identity Service Center Request Access wizard to provide user accesses, such as role membership, accounts, and groups. The wizard provides a unified catalog of access that you can use.

Before you begin

Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access to this task.

The system configuration, such as access catalog information and provisioning policies, affects the users and accesses that can be selected in this flow.

Follow your organization process for any operations or permissions to make sure that your request is valid.

About this task

The account form in the request access task does not display the group information for a user. To view and edit the group-related access assignments, define a group as access, and then use the access management flows such as View Access, Request Access, or Edit or Delete Access.

Use the Request Access wizard to request one or more accesses for a user from the unified catalog of accesses. The wizard supports batch requests by building up a list of items to request before you go to the next step. For example, a user moves into a new role, and the manager wants to give the user the access to multiple systems or applications.

Procedure

1. From the Identity Service Center Home page, click **Request Access** to display the Select user page.
2. On the Select user page, select a user to display the Select accesses page. The available users are displayed in a grid of cards view.
3. On the Select accesses page, select one or more accesses for the selected user.

   Note: A message is displayed if you exceed the maximum limit that is set for selecting the access. If no maximum limit is set, the default access selection limit is 25.

   The **Request summary** field displays an updated summary about the selected user, accesses, errors, warnings, or information messages about the access selections. Click **Request summary** to open and view the details.

   Request access for
   Displays the name of the selected user.

   Request access to
   Displays the selected accesses for the selected user.

   If you want to start with your request again, then click **Cancel my request**.
4. Click **Next** to open the Provide required information page.
5. Provide a brief description or justification about your business requirement for the access items that you selected to request for the user.
6. Depending on the configuration, click **Provide account information**, if it is displayed, to open the Account information page. Specify the additional information that is necessary for your request, such as personal information about the requester, or necessary resource-specific information.

   Note: For non-compliant values or validation errors in any Identity Service Center console fields, click outside the field or tab to view or display the updated hover or hint text.

   After the account information is entered, click **Continue request** to return to the Provide required information page.
7. Click **Submit**. A message is displayed to indicate a successful submission or any submission errors.

What to do next

View the confirmation and status of your submitted request in the View requests page. To do so, go to **Home** > **View Requests**.

Request more accesses for the selected user, or specify new accesses for another user.

Requesting access for an employee with an existing account in the server

This scenario describes how to request access for an employee with an existing account.

Procedure

1. On the home page, click **Request Access**.
2. On the Select user page, select the name of the user that requires access.

3. On the Select access page, select **Accounting Plus**.
4. Click **Next**.

   On the Provide required information page, a justification is required.
5. Enter the justification for the request.

   If the user you selected already has an account on the application server, you are not prompted to create a new account. If the access is granted, the account is associated with the access.
6. Click **Submit**.
7. Reload the page and the request status changes to **Success**.

Selecting a different user or set of access rights after a request flow is initiated

Use the Request Access page to select a user and request one or more accesses from the unified catalog of access options. You can customize your requirements by changing a user or access selection.

Before you begin

Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access to this task.

The system configuration, such as access catalog information and provisioning policies, affects how you select the users and access rights in this flow.

Follow your organization process for any operations or permissions to make sure that your request is valid.

About this task

You can change a user or access selection even after you provide the required information for an earlier access request.

Procedure

1. From the Identity Service Center Home page, click **Request Access**.
2. On the Select user page, select a user. The Select accesses page opens to display the access options that the selected user is entitled and allowed to see.

   If you return to the Select user page to change the user, a message shows. It informs you that you lose any access that you selected in the Select accesses page. The message provides you with an option to discard or retain the access for the user.

   If you click **Yes** on the message, the selected access rights on the Select accesses page are discarded.

   If you click **No** on the message, the user change is discarded.
3. On the Select accesses page, select one or more access rights for the user.

   The Request summary field displays an updated summary about the selected user, access rights, errors, warnings, or information messages about the access selections.
4. Click **Next** or select **Provide required information** from the workflow sequence map at the top of the page.
5. Enter a justification for your request. You can provide the account form information, passwords, and other information.

> **Note:** For non-compliant values or validation errors in any Identity Service Center console fields, click outside the field or tab to view or display the updated hover or hint text.

6. Click **Submit**.

Results

View the confirmation and status for your submitted request in the View requests page. You can also bookmark the page to revisit it later.

Sorting in the Identity Service Center

The Identity Service Center Select user page displays the list of employee cards that the logged-in user is authorized to view. The person card displays the employee picture, if available, name, email address, and title. The contents can also be customized.

Procedure

1. From the Select user page menu, search for a user. Whatever you enter in the text box is matched against the name, email or title of the person.

   Search results depend on whether the entry is found in the system.

2. Type the text in the **Search** field, and click **Enter**.

   The list of employee cards can be sorted by name, mail, or title in the ascending or descending order.

3. Locate **Sort By**. Click **Name**, **Mail**, or **Title**. The order of the employee card list changes. Click the name again if you want to sort the list in another order.

   Note: For left-to-right text orientation, such as English or French, the **Sort By** link is on the upper right of the screen. For right-to-left text orientation, for example, Hebrew or Arabic, the **Sort By** link is on the upper left of the screen.

Custom label translation overview

The topic provides information about how the translated custom labels are displayed.

To enable the translation of a label description, the prefix $ is added to the description string and the translation for that property is provided in *ISIM_HOME*/data/CustomLabels.properties file.

Regardless of the locale that is set while a user enters the custom label description, only the custom label string that is defined in the *ISIM_HOME*/data/CustomLabels.properties file is displayed.

The label string that is defined in the *ISIM_HOME*/data/CustomLabels.properties file takes precedence over the locale that is selected by a user. If a custom label is not defined in the *ISIM_HOME*/data/CustomLabels.properties file, the English label is displayed by default even though the user specifies a different locale.

Searching for accesses on the Select Access page

The Select access page displays the list of authorized access for the selected user. Each access card has the access name, description, category, and default icon that represents the category. Some accesses include a badge. The access card contents can also be customized.

Procedure

1. From the Select accesses page menu, type the search string in the **Search** field.

   By default, the returned result contains the matching text in access name, description, or badge.

2. Click **Enter**. The search result changes.

   The list of all the access categories is displayed under the **Search** field.

3. Click a category and see that the breadcrumb is updated to include the selected category name. The list of access cards is updated to include only those names that are defined in the specific category.

   You can drill down through the category hierarchy.

4. Depending on the configuration, you can click the breadcrumb names of the categories to go up in the category hierarchy. For example, you can click **All categories** to update the search to show all accesses that match the search filter regardless of the access category.

View requests in the Identity Service Center

You can view all your requests that are made by you. You can also view the requests that are made on your behalf.

You can view your requests within the specified time period. The request lists the type of request, requester, request number, and status of the request.

If the request is submitted on your behalf, you can view the requester.

You can also view details about all your requests that are made for and by you.

Viewing request status in the Identity Service Center

View the status and details of requests that are submitted from the Identity Service Center.

Procedure

1. From the Identity Service Center Home page, click **View Requests**.
2. Use the search and sort options to limit the amount of request information that is displayed.
3. To view the details of the individual accesses, click the **View Details**. The **View Request Status Details** page opens.

   You can also view the details about the access requests that are submitted after you edit or delete accesses. By default, the requests on the page are sorted in an order such as `Pending`, `Not fulfilled`, and `Fulfilled`.

   In the **Request Details** section, you can view status of the individual access request. The **Information Provided with the Request** section displays a read-only copy of the information that you supplied on the Provide Required Information page when you submitted the request. You cannot change this information.

The **Activities and Decisions** section indicates any pending actions that must be taken, such as approvals. It lists the approval status, approver name, and comments added by the approver.

What to do next

If necessary, proceed with the other tasks such as request more accesses, edit, or delete accesses.

Narrowing down search results by using specific search control options

Use the search control options to narrow your search on entities such as persons, accesses, groups, roles, services, and organizational containers in the Identity Service Center. The search returns information that matches the specified search criteria.

The Identity Service Center provides a mechanism to select one or more items from a list for doing a basic or advanced search. Queries are not case-sensitive. Search results depend on whether or not the entry is in the system.

You can narrow your search in these ways:

Simple or basic search
Click the **Search** icon next to the **Search** field to display a list of top three results. You can also type a search text or a portion of the string in the **Search** field to retrieve the results. The results are displayed in a card format. Click a specific card or press **Enter** to select and add it to the list. You can click the selection to view the card information.

Note: If the search uses a non-string data type attribute such as Boolean or integer, the text-based search is not supported. Click the **Search** icon to retrieve all the results without filtering that is based on the search text.

To delete a selected item, click the **Delete** icon.

To see a complete list, click **See all *NNN* results**, where *NNN* is the number of search items.

If the list contains more than five selected items, then the **And *NNN* more** link is displayed, where *NNN* is the number of search items.
To view a full list of the selected items, click the **And *NNN* more** link. The Full List window is displayed. If the full list contains multiple pages, then do one of the following actions:

- Click **Next** to go to the next page.
- Click **Previous** to go to the previous page.
- Click the number of the page to view that page.

To remove one or more selected items, click **Remove**.
Click **OK** to remove your selections and close the Full List window. Click **Cancel** to revert your selections.

To see a complete search list, click **See all *NNN* results**, where *NNN* is the number of search items.

Advanced search
With your specified search text in the **Search** field, click **Advanced search** or **See all *NNN* results** to open the Advanced Search window.

When you click **See all *NNN* results**, your specified search text, the selected search attributes, and the **Contains** operator is retained in the Advanced Search window. When you click **Advanced search**, the search text is not retained in the Advanced Search window.

The Advanced Search window contains the following filter options:

Attribute
Select an attribute such as `mail`, `organization`, `telephone`, or other attributes for your search.

> **Note:** You cannot sort or filter your search on the `name` attribute.

Operator
Select an operator such as **Contains**, **Does not contain**, **Equals**, **Greater than**, or **Less than** that links the **Attribute** and **Value** fields together.

> **Note:** In an advanced search, if a non-string data type attribute such as Boolean or integer is searched, do not use the operators **Contains** or **Does not contain**. For a Boolean type, the only supported operator is **Equals**. For an integer type, the supported operators are **Equals**, **Less than**, and **Greater than**.

Value Type a value for the search attribute.

You can use these buttons:

Search
Click to display a list of search results that are based on the selected search attribute. The list of search items is displayed in a table format. The column names depend on what attributes you configured to display in the list.

Select Click to select a search item from the result list. The label changes to **Selected**, and the Advanced Search window closes to prevent you from selecting more than one search item. The **Select** button is not enabled until you select another search item.

To select another search item in the result list, click **Select**. The label for that search item changes to **Selected** and the label for the previous search item changes to **Select**.

Add Click to add a search item from the result list. The label changes to **Remove**.

Remove
Click to remove a search item from the result list. The label changes to **Add**.

Click **Close** to exit from the Advanced Search window and add the selected items to the basic search results list.

If you encounter any errors from a search operation, then complete some actions to correct the errors and try the operation again. For example:
- Review or verify whether the search query is correct or valid.
- Verify the search context.
- Determine whether the system is running correctly.
- Determine whether you are authorized to do the search operation.

You can also contact your site administrator for more clarifications.

Managing approval activities

You can use the Identity Service Center to approve or reject requests that are assigned to you.

Before you begin

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

About this task

An activity is an action item that is displayed in your activities list as part of a workflow process and requires your action. You can use the Identity Service Center to view your activities, approve, and reject approval requests.

Note: You can view only those attributes for which you are granted read permission.

For non-approval activities, when you click the activity card, you are redirected to the Self-Service console to complete the activity. Non-approval activities are marked with an icon and include

> Requests for information
>
> Separation of duty violations
>
> User recertifications
>
> Compliance alerts
>
> Work orders

Procedure

1. Log on to Identity Service Center.
2. Click **Manage Activities** > **My Activities**. The Manage Activities and Decisions page is displayed.
3. Optional: You can filter the activities that are displayed. You can enter a string in the **Search** field to search for activities that contain the string. You can also use the quick search categories to narrow the list of activities that are displayed.
4. Select the approval activity.
   - Click the approval activity card to take immediate action.
   - Click **View Details** to view more information about an approval request before you act on the request.
5. Type the reason for your decision and any additional comments.
6. Complete the approval activity.
   - Click **Approve**.
   - Click **Reject**.

   Your action is processed and the activity card is updated appropriately.

What to do next

You can continue to work on your activities, review previously completed activities, or exit from the Manage Activities and Decisions page.

Managing multiple activities

You can use the Identity Service Center to approve or reject simultaneously multiple requests that are assigned to you.

Before you begin

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

About this task

An activity is an action item that is displayed in your activities list as part of a workflow process and requires your action. You can use the Identity Service Center to approve and reject multiple approval activities. When you use this option, you provide a single justification and the same operation is performed on all the selected items.

Note: You can view only those attributes for which you are granted read permission.

For non-approval activities, when you click the activity card, you are redirected to the Self-Service console to complete the activity. Non-approval activities are marked with an icon and include

Requests for information

Separation of duty violations

User recertifications

Compliance alerts

Work orders

Procedure

1. Log on to Identity Service Center.
2. Click **Manage Activities** > **My Activities**. The Manage Activities and Decisions page is displayed.
3. Optional: You can filter the activities that are displayed. You can enter a string in the **Search** field to search for activities that contain the string. You can also use the quick search categories to narrow the list of activities that are displayed.
4. Click **Select Multiple**. The selectable activities are displayed with a check box.
5. Select the approval activity.
   - Click the check box for each approval activity that you want to take the same action on.
   - Click the check box for a single approval activity and click **Select All on this Page** to select all similar activities.
6. Type the reason for your decision and any additional comments. The justification is applied to each of the selected activities.
7. Complete the approval activity.
   - Click **Approve**.
   - Click **Reject**.

   Your action is processed and the activity cards are updated appropriately.

What to do next

You can continue to work on your activities, review previously completed activities, or exit from the Manage Activities and Decisions page.

Delegating your activities

When you are not available to manage your activities, you can delegate them to another user. The delegation will apply only to future activities.

Procedure
1. From the Identity Service Center home page, click **Delegate Activities**.
2. On the Delegate My Activities page, click the **Delegate Activities to** field to locate the user. You can also type in the field to locate the user.
3. Click the full name of the user that you want to select.
4. Select the time period for delegating your activities, specifying a start date in the **Start Date** field and an end date in the **End Date** field.
5. Click **Save Delegation Schedule** to save your delegation schedule.
6. On the Delegation Schedule Saved page, verify your changes. Act on one of these options.
    - If no changes are required to the saved delegation schedule, return to the home page.
    - To edit the delegation schedule:
        a. Click **Edit or Delete Delegation Schedule**.
        b. Edit the fields that you want.
        c. Click **Save Changes**.
    - To delete the delegation schedule:
        a. Click **Edit or Delete Delegation Schedule**.
        b. Click **Delete**.

What to do next

Create a delegation schedule, or edit or delete the existing delegation schedule.

Editing a user profile

You can edit the information that is contained in a user profile. You can also review the modification details and choose to discard the changes.

Before you begin

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

About this task

The account form in the edit profile task does not display the role information for a user. To edit the role-related access assignments, use the alternative access management flows such as Request Access, Edit or Delete Access.

Procedure
1. Log on to the Identity Service Center.
2. From the Identity Service Center Home page, click **View and Edit Profile**.
3. Take one of the following actions:
   - If you are on the Select User page, click the user for whom you want to edit the profile.
   - If you are editing profile for yourself, click **Select me** in the **Quick Select** menu.

   In the **Request Summary**, the selected user name is displayed.
4. In the Profile Details page, edit the attributes.
5. If you edited some attributes, click **Save and Continue**.
6. Provide a brief justification for the request.
7. Optional: You can discard the changes by clicking **Undo Edit**.
8. Optional: Review the modification details by clicking **Review Changes**.
   - Click the toggle icons to change the views of the modification details.
   - Click **Back**.
9. Click **Submit**.

Results

The request to edit a user profile is submitted.

What to do next

Edit more user profiles or view the status of your request.

Changing the password

When you change the password, you can change it for one, more, or all accounts. If password synchronization is enabled, the password is changed for all of individual accounts automatically. If password synchronization is not enabled, select the accounts for which you want to change the password.

Procedure
1. From the Identity Service Center home page, click **Change Password**.
2. Take one of the following actions:
   - If you are on the Select User page, select the user for whom you want to change the password.
   - If you are changing the password for yourself, click **Select me** in the **Quick Select** menu.

   In the **Request Summary**, the selected user name is displayed.
3. View or select your accounts.
   - If password synchronization is enabled, a list of individual accounts up to the maximum search limit is displayed. The password change applies to all individual accounts. The individual accounts that are not listed are also changed.
   - If password synchronization is not enabled, you must select each account to change the password.
4. Complete one of the following options.

- If you want a system to generate a password:
  a. Ensure **Generate a password for me** is selected.
  b. Click **Submit**.
- If you want to type in the new password:
  a. Select **Allow me to type a password**.
  b. At **New password**, type a new password.
  c. At **Confirm new password**, type the new password again.
  d. Click **Submit**.
- If the **Enable password editing** box is cleared in the administrative console, then you do not see the **Generate a password for me** and **Allow me to type a password** options in the Identity Service Center. By default, the system generates the new password. Click **Submit**.

5. Verify the change password information and the status of the request.

Results

Request to change the password is submitted.

What to do next

Change more passwords or view the status of the requests that are already submitted.

Changing and resetting forgotten passwords

Depending on how a system administrator configured the system, when you forget your password, you can change it or have the system reset it. You must answer one or more forgotten password questions correctly.

Before you begin

You must have previously specified your forgotten password information before completing these steps.

About this task

When you forget your password, you must answer the challenge questions correctly and change your password. The new password replaces the old password for your account. Depending on how your system is configured, you can either specify a new password or have the password automatically generated by the system. The generated password is sent to the e-mail address that is specified in your personal profile. Depending on how your system is configured, an email contains either the password or a link that contains the password. If the system is configured to receive an email with a link to change the password, you must enter the shared secret to open that link to change the password.

If password synchronization is enabled and your account is an individual account, the password is changed for all of your individual accounts.

To change your password when you forgot it:

Procedure

1. From the Identity Service Center Login page, type your user ID, and then click **Forgot your password?**

2. On the Forgot Your Password page, answer the forgotten password questions, and then click **Submit**.
   - If the questions are answered correctly, your system is configured to automatically generate a new password, and send the password to email address, then the Forgotten Password: Email Sent page opens. The new password is sent to you by email. You must use this password to log in.
   - If the questions are answered correctly, your system is configured to automatically generate a new password, and send a link that contains the password, then the Forgotten Password: Email Sent page opens. A link that contains the password is sent to you by email. You must specify the shared secret to open that link to change the password.
   - If the questions are answered correctly and your system is configured for you to specify a new password, you are prompted to change the password. You can view the accounts that are affected by the password change. Follow the steps that are provided to change the password, and click **Submit**.
   - If the forgotten password questions are not answered correctly, you receive an error message. You cannot access the system until you remember your password or answer the questions correctly. If you can do neither, contact your system administrator to reset your password.

3. Click **Log In** to return to login page.

Results

The reset or change of the forgotten password is complete successfully.

Complex password policy rules overview

The topic provides information about the complex password policy rules and how the cumulative password rules are displayed in the Identity Service Center.

A password policy defines the password rules that are used to determine whether a new password is valid.

The password rules that are displayed in the Identity Service Center user interface takes the following flow.
- When a user selects an account, the password policy rules for that account are displayed.
- If user selects multiple accounts, Identity Service Center combines policies for the accounts that user selected and displays the password rules in cumulative format.
- If the password policy associated with an account that user selected contains the complex password rules selected, then the password requirements also contain the rules that are associated with the complex password rules. Complex password policy rules contain four categories out of which three categories must be satisfied for a valid password. Following are the four categories for the complex password policy.
  - Uppercase letter [A-Z]
  - Lowercase letter [a-z]
  - Number [0-9]

– Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- The cumulative list of password rules is displayed in the **Password Requirements** section of the Identity Service Center user interface.

There might be password rule conflicts. The first password policy that is associated with an account sets the maximum length to 2 characters. Another password policy that is associated with the selected account enables the password complexity rule. In this scenario, a valid password cannot be created that satisfies both the conditions. That means to create the valid password, the first policy requires maximum 2 characters and another policy with the complex password rule requires minimum 3 characters.

Edit or delete accesses

Based on your permissions, you can edit or delete the accesses in the Identity Service Center for yourself, another user, or both.

The initial user interface page is based on the permissions that you are granted.

For example, in the Edit and Delete Access wizard, if you edit or delete accesses for:
- Yourself: If you are editing or deleting accesses for yourself, click **Select me** in the **Quick Select** menu. You are directed to the **Select Accesses** page.
- Another user: You are directed to the **Select User** page. There is no option to select yourself.
- Yourself or another user: You are directed to the **Select User** page.

For the detailed steps to edit or delete the accesses,
- See "Editing accesses in Identity Service Center."
- See "Deleting accesses in the Identity Service Center" on page 60.

Editing accesses in Identity Service Center

Use the Identity Service Center Edit and Delete Access wizard to edit the accesses for yourself or another user.

Before you begin

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

About this task

The account form in the edit access task does not display the group information for a user. To view and edit the group-related access assignments, define a group as access, and then use the access management flows such as View Access, Request Access, or Edit and Delete Access.

Procedure

1. Log on to the Identity Service Center.
2. From the Identity Service Center Home page, click **Edit and Delete Access**.
3. Take one of the following actions:

- If you are on the Select User page, click the user for whom you want to edit accesses.
- If you are editing accesses for yourself, click **Select me** in the **Quick Select** menu.

In the **Request Summary**, the selected user name is displayed.

4. In the Select Accesses page, click **Edit** for the access items that you want to edit.

   In the **Request Summary**, the number of items in the cart is increased for each access that is edited.

5. If you edited some attributes, click **Save and Continue**.

6. Click **Next**.

7. Provide a brief justification for the request and review the choices for editing the access.

8. Optional: Discard the changes by clicking **Undo Edit**.

9. Optional: Review the modification details by clicking **Review Changes**.
   - Click toggle button to view the modification details in two different formats.
   - Click **Back**.

10. Optional: Click **Request Summary** to and view the summary details. An option to discard the edit changes is also on the summary details page.
    - Select the access for which you want to discard the changes and click **x**.
    - To start your request again, click **Cancel My Request**.

11. Click **Submit**.

Results

The request to edit accesses is submitted.

What to do next

Edit more accesses or view the status of your request.

Deleting accesses in the Identity Service Center

Use the Identity Service Center Manage Access wizard to delete the accesses for yourself or another user.

Before you begin

Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access.

Procedure

1. Log on to the Identity Service Center.

2. From the Identity Service Center Home page, click **Edit and Delete Access**.

3. Take one of the following actions:
   - If you are on the Select User page, click the user for whom you want to delete accesses.
   - If you are deleting accesses for yourself, click **Select me** in the **Quick Select** menu.

   In the **Request Summary**, the selected user name is displayed.

4. In the Select Accesses page, click **Delete** for the access items that you want to delete.

   In the **Request Summary**, the number of items in the cart is increased for each access that is deleted.

5. Click **Next**.

6. Provide a brief justification for the request and review the choices for deleting the access.

7. Optional: You can discard by clicking **Undo Delete**.

8. Optional: Click **Request Summary** to view the summary details. An option to discard the delete changes is also on the summary details page.

   • Select the access for which you want to discard the changes and click **x**.

   • To start your request again, then click **Cancel My Request**.

9. Click **Submit**.

Results

The request to delete accesses is submitted.

What to do next

Delete more accesses or view the status of your request.

Defining the filter identifier for REST search service

To use a specific filter configuration for a request, you can provide the filter identifier as URL query parameter. The filter identifier must be configured in the `custom/rest/searchfilter.json` file. The REST Service uses the corresponding filter configuration to create the filter expression. The filter identifier is useful when a REST endpoint is started for different REST functions.

About this task

By default, the REST search service returns all the data for an entity. To get a specific search result, you must customize the search operation by defining the filter identifier for the REST search service. Complete the following steps.

Procedure

1. Access `http://`*`hostname`*`:`*`port`*`/itim/rest/dictionary` to find the REST service endpoint key.

2. Define the filter identifier text for the REST service endpoint key in the `isim/data/rest.properties` file.

3. Add the filter identifier details in the `custom/rest/searchfilter.json` file. For example, if you define the filter identifier in the `isim/data/rest.properties` as `customsearch`, then you can add the following details in the `custom/rest/searchfilter.json` file.

```
"customsearch": {
    "filterTemplate": "(&(requester=${requester})(${filterExpression}))",
    "joinOperator": "&",
    "multivalueJoinOperator": "|",
    "comparisonOperator": ">=",
    "baseFilter": "(!(uid=${systemUser.owner.uid}))",
    "allowWildcard": "false"
```

Results

The filter identifier is defined according to your requirement. Use the filter identifier `customsearch` as a URL parameter for the REST search service.

Example

For more information about how to use filter identifier in the request URL, see examples in the Filter configuration for REST search services.

Single sign-on scenario in the Identity Service Center

In the *ISIM_HOME*/data/ui.properties file, the properties `enrole.ui.ssoEnabled` and `enrole.ui.taiEnabled` define the single sign-on behavior.

When a single sign-on is enabled by editing these properties and a user changes the password or sets the answers for the challenge questions, the Identity Service Center does not prompt for a system password.

Chapter 7. Help desk scenarios

These scenarios demonstrate some of the administrative tasks that a help desk assistant would do in IBM Security Identity Manager.

Commonly, users call the help desk because they forgot their password or because an account is locked. The help desk assistant can unlock the account or verify the user's identity and then reset their password. The new password is typically e-mailed to the user. If the password is for the e-mail account itself, there are other options that you can set within IBM Security Identity Manager.

Changing a user password

This scenario describes how to change passwords for other users as a help desk assistant in IBM Security Identity Manager.

Before you begin

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

About this task

Janice Helpdesk works as a help desk assistant for the insurance company, assisting users who use resources and cannot find or maintain these resources. In this scenario, Mike Sysadmin, a Security Identity Manager administrator, forgets a password and requires assistance. Janice verifies the necessary personal information and resets or changes the password.

To change a user password in Security Identity Manager, complete these steps:

Procedure

1. Log in to the administrative console user interface as user `jhelpdesk` with password `secret`.
2. From the navigation tree, click **Change Passwords**.
3. On the Select a User page, type `Mike Sysadmin` in the **Search information** field and click **Search**. Select **Mike Sysadmin** and click **Continue**. The user's personal information can be viewed in read-only form with the hyperlink under the user's name. Use this information to verify the user's identity.
4. On the Change Passwords page, complete these steps:
   a. Select **Allow me to type a password**. We use this option for this example. However, for security purposes, it is more likely you would want to generate a random password.
   b. In the **Password** field, type `secret`.
   c. In the **Confirm password** field, type `secret`.
   d. Click **Submit**.

   As a second check on the user's identity, the password is typically sent to the email address that the user has on record. The password is not read aloud during the phone conversation.

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

Chapter 8. Auditor scenarios

These scenarios demonstrate some of the administrative tasks that an auditor would do in IBM Security Identity Manager.

Verifying that the only the right users have access to business critical applications is an important part of auditing compliance to a number of regulations. For example, compliance is required by a regulation such as Sarbanes-Oxley. IBM Security Identity Manager has a number of reports you can generate to help with verification.

Generation of a report

This scenario demonstrates how to generate a report in IBM Security Identity Manager.

Generating a report

This scenario describes how to generate reports as an auditor in IBM Security Identity Manager.

Before you begin

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

About this task

Jeff Auditor is a member of the audit team, and also has other responsibilities within the company. Jeff is running a report to generate a report and view information about users and their accounts in the system. The report helps Jeff ensure that the system meets corporate regulatory requirements.

To generate a report in Security Identity Manager, complete these steps:

Procedure

1. Log in to the administrative console user interface as user `jauditor` with password `secret`.
2. From the navigation tree, click **Reports** > **User and Account Reports**.
3. On the Options page, click **Individual Accounts**.

   You might see a warning message about data report synchronization.
4. On the Individual Accounts page, click **OK**.

   This report takes several minutes to generate. Data synchronization must be run by an administrator before generating a report, or no data is displayed.
5. On the Success page, click **Close**.

Generation of Cognos reports

The following scenarios demonstrate how to generate Cognos reports in IBM Security Identity Manager.

For the Cognos Reporting scenarios, the main personas are:

- **Mark Pond** – Auditor. Mark must view all the audit data for the finance department and generate reports depending on the requirements
- **Laura Whelan** – Administrator. Laura must inspect all the kinds of operations that are done on shared or privileged IDs in the organization.

Generating an auditing history report

This scenario describes how to generate an auditing history report. Mark Pond wants to monitor all the account audit actions such as add, delete, suspend, restore, and orphan in the JK Enterprises finance sub-organization over a period of time. **Solution**: Mark can run the *Audit History Report* for accounts.

Procedure

1. Open the Cognos® URL `http://IP address or host name/ibmcognos/cgi-bin/cognos.cgi` in a browser.
2. Click the **SAReportingModel_6.0** link on this page. It displays a list of static reports.
3. Click the **Audit History Report** link.
4. From the **Audit Report type** drop-down menu, select **Account**.
5. When you are prompted to provide the parameters for the report, enter the values for the filters based on your requirements.

   To see the list of available values under a particular filter, enter `%` in the text field, then click **Search**.

   Select the values from the list and click **Insert** to add them to the **Choice** list.

   Click **Next** to go to the next filter selection page, if any.
6. When you are done with the parameter value selection, click **Finish**.

   A summary page lists the selections you made for the filters. There are page browsing links (such as **Page Down**, **Page Up**, **Top**, **Bottom**) available at the bottom of the page.
7. Click the **Page Down** link to go to the next page of the report.

   The generated report shows all the accounts that were added, deleted, suspended, restored, and orphaned over a period of time.

Generating a report to check the status of the provisioned accounts

This scenario describes how to generate a report to check the status of the provisioned accounts. Laura Whelan wants to administer all the accounts that were provisioned on the services to check the state or status of the accounts in the JK Enterprises finance sub-organization. **Solution**: Laura can run the *Account Status Report* to check the state or status of all the accounts in the JK Enterprises finance sub-organization.

Procedure

1. Open the Cognos URL `http://IP address or host name/ibmcognos/cgi-bin/cognos.cgi` in a browser.
2. Click the **SAReportingModel_6.0** link on this page. It displays a list of static reports.
3. Click the **Account Status Report** link on this page.
4. When you are prompted to provide the parameters for the report, enter the values for the filters based on your requirements.

To see the list of available values under a particular filter, enter % in the text field, then click **Search**.

Select the values from the list and click **Insert** to add the values to the **Choice** list.

Click **Next** to go to the next filter selection page, if any.

5. When you are done with the parameter value selection, click **Finish**.

A summary page lists the selections you made for the filters. There are page browsing links (such as **Page Down**, **Page Up**, **Top**, **Bottom**) available at the bottom of the page.

6. Click the **Page Down** link to go to the next page of the report.

The generated report shows the status or states of all the accounts within the finance sub-organization.

Generating a report to view policy violations and exemptions

This scenario describes how to generate a report to view policy violations and exemptions in the company. Laura Whelan wants to view the Separation Of Duty policy violations and exemptions over a period of time. **Solution**: Laura can run the *Separation of Duty Policy Violation Report*.

Procedure

1. Open the Cognos URL `http://IP address or host name/ibmcognos/cgi-bin/cognos.cgi` in a browser.
2. Click the **SAReportingModel_6.0** link on this page. It displays a list of static reports.
3. Click the **Separation of Duty Policy Violation Report** link.
4. When you are prompted to provide the parameters for the report, enter the values for the filters based on your requirements.

To see the list of available values under a particular filter, enter % in the text field, then click **Search**.

Select the values from the list and click **Insert** to add the values to the **Choice** list.

Click **Next** to go to the next filter selection page, if any.

5. When you are done with the parameter value selection, click **Finish**.

A summary page lists the selections you made for the filters. There are page browsing links (such as **Page Down**, **Page Up**, **Top**, **Bottom**) available at the bottom of the page.

6. The generated report shows the Separation of Duty policy violations and exemptions over a period of time for the finance sub-organization.

Generating a report to view the IBM Security Identity Manager environment details

This scenario describes how to generate a report to view the IBM Security Identity Manager environment details. Laura wants to look at the summary of the IBM Security Identity Manager (ISIM) environment. She wants to view the detailed information about the key activities and size metrics. She also wants to see how large the IBM Security Identity Manager environment is in her organization. **Solution**: Laura can run the **ISIM Environment Dashboard** to get information about the entities such as roles, accounts, provisioning policies, resources, separation of duty policy violations, and users.

Procedure

1. Open the Cognos URL http://*IP address or host name*/ibmcognos/cgi-bin/
cognos.cgi in a browser.
2. Click the **SAReportingModel_6.0** link on this page. It displays a list of static
reports.
3. Click the **ISIM Environment Dashboard** link.
4. The dashboard shows the IBM Security Identity Manager environment details
such as accounts, provisioning policies, resources, roles, separation of duty
policy violations, and users.
5. Click the chart bar associated with an entity to view more information about
the specific entity.

Customizing Cognos reports

This scenario describes how to customize reports by using the Cognos Reporting
framework. IBM Security Identity Manager, version 6.0, fix pack 2, provides some
default reports that cover critical use cases. Aside from the static reports, you can
easily customize reports in Cognos.

Procedure

1. Open the Cognos URL http://*IP address or host name*/ibmcognos/cgi-bin/
cognos.cgi in a browser.
2. On the home page, click **Launch** and then select **Cognos Workspace Advanced**.
3. Select the **SAReportingModel_6.0** package. A new window opens an advanced
workspace for customizing reports.
4. Click **Create New**.
5. Select **List** template, then click **OK**. A canvas opens. Select the items that you
need from the right panel to customize your report.

    The right panel shows the IBM Security Identity Manager metadata model. The
    model is divided based on customer values. Each of the model is divided into
    two categories, such as configuration and audit.

    The Audit category has all the information that is required to generate audit
    report. The configuration model has information that you can use to design
    configuration-related reports.

Customizing the report to show role access

This scenario describes how to customize a report to show role access. Laura
Whelan wants to generate the Role access definition report to list all the users who
have access to a role that is defined as an access.

About this task

Note: This scenario can also be used with access configuration namespace. The
access configuration namespace gives a unified view of all accesses that are
defined in an organization.

Procedure

1. Open the Cognos URL http://*IP address or host name*/ibmcognos/cgi-bin/
cognos.cgi in a browser.
2. On the home page, click **Launch** and then select **Cognos Workspace
Advanced**.

3. Select the **SAReportingModel_6.0** package. A new window opens an advanced workspace for customizing reports.

4. Click **Create New**.

5. Select **List** template, then click **OK**. A canvas opens. Select the items that you need from the right panel to customize your report.

6. Create a report.

7. Go to **Roles > Role Configuration > Role** query subject.

8. Drag **Role Name** and **Role Type**.

9. Expand **Role Members** query subject, then drag **Role Member Full Name**.

10. Expand **Role** query subject, and then drag **Role Access Enabled**, **Role Common Access Enabled**, and **Role Access Type**.

11. Select any record from the **Role Member Full Name** column. Then, follow the menu **Structure > Group/Ungroup**.

12. Group the **Role Name** column. When you complete these steps, provide a name for the report and save it. You can run the report again at a later time.

Customizing the report to show user recertification history

This scenario describes how to customize a report to show user recertification history. Mark Pond wants to know users who got recertified in a certain time.

Procedure

1. Open the Cognos URL `http://IP address or host name/ibmcognos/cgi-bin/cognos.cgi` in a browser.

2. On the home page, click **Launch** and then select **Cognos Workspace Advanced**.

3. Select the **SAReportingModel_6.0** package. A new window opens an advanced workspace for customizing reports.

4. Click **Create New**.

5. Select **List** template, then click **OK**. A canvas opens. Select the items that you need from the right panel to customize your report.

6. Create a report.

7. Go to **Recertification > Recertification Audit > User Recert History** query subject.

8. Drag **User Recert History Person Business Unit Name**.

9. Drag **User Recert History Person Name**.

10. Drag **User Recert History Prcess Submission Time**, **User Recert History Process Completion Time** and **User Recert History Process Recertifier Name**.

11. Expand **User Recert Account** and drag **User Recert Account Status**.

12. Expand **User Recert Group** and drag **User Recert Group Status**.

13. Expand **User Recert Role** and drag **User Recert Role Status**.

14. Expand **User Recert History** and drag **User Recert History Comments**.

15. Select any record in the **User Recert History Person Business Unit Name** column and follow the **Structure** > **Group/Ungroup** menu to group Business unit names. When you complete these steps, provide a name for the report and save it. You can run the report again at a later time.

Index

IBM ®

Printed in USA