INSTITUTE OF COMPUTER TECHNOLOGY
B-TECH COMPUTER SCIENCE ENGINEERING 2025-26
SUBJECT: IDENTITY ACCESS MANAGEMENT

NAME: Rahul Prajapati
ENRLL. NO: 23162171020
BRANCH: CYBER SECURITY
BATCH: 52

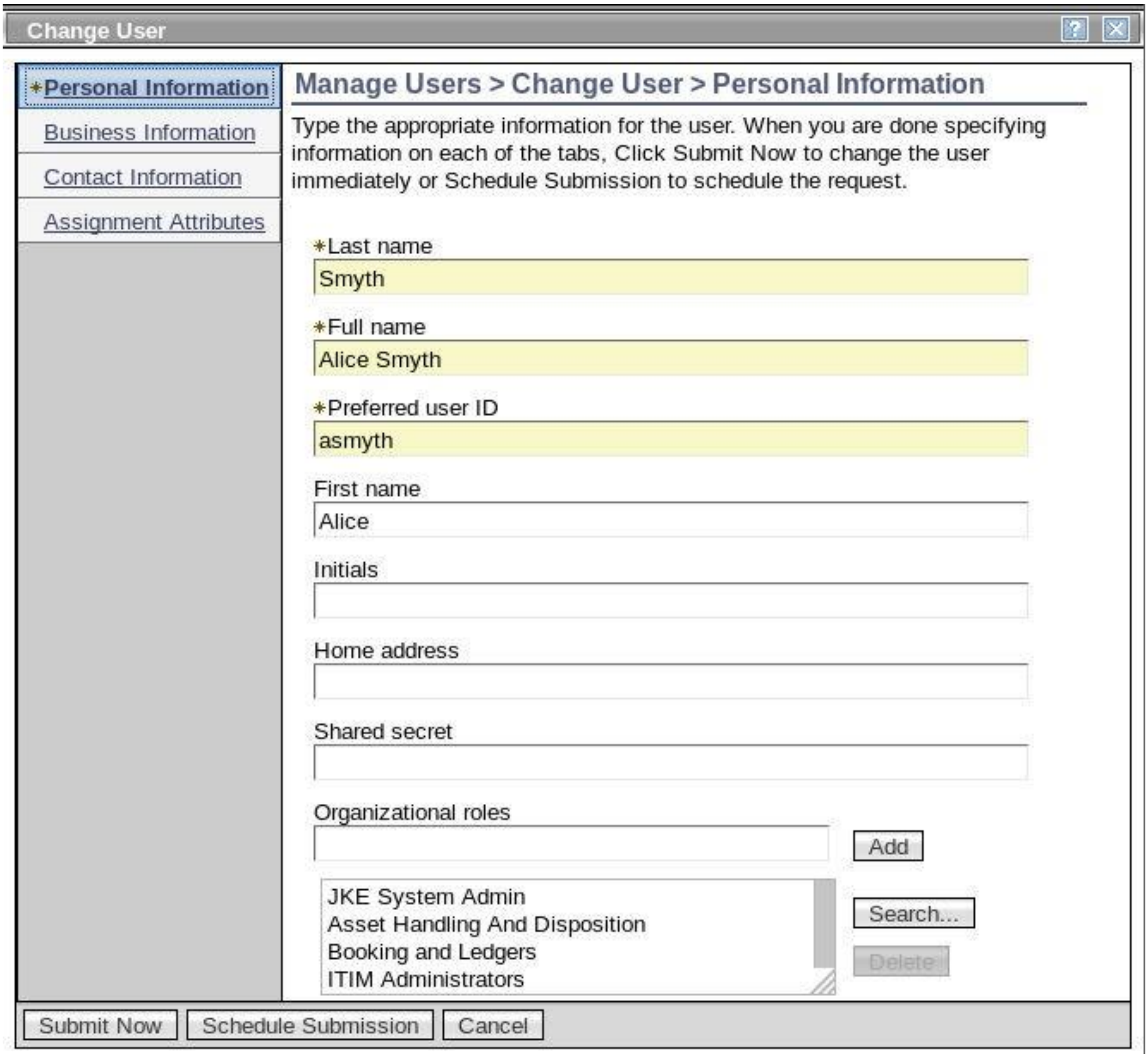
Lab 12: Provisioning resources exercises

Exercise 7.1 – Adding Users to a Static Role

Objective: Assign users to organizational roles before creating provisioning policies.

Task 1: Assign JKE System Admin Role

1. Log in to ISIM as itim manager.
2. Navigate to **Home** $\rightarrow$ **Manage Users**.
3. Search for and select **Alice Smyth** $\rightarrow$ **Personal Information** tab.
4. Add the **JKE System Admin** organizational role to Alice Smyth.
5. Click **Submit Now** $\rightarrow$ **Close**.



Manage Users > Change User > Personal Information

Type the appropriate information for the user. When you are done specifying information on each of the tabs, Click Submit Now to change the user immediately or Schedule Submission to schedule the request.

*Last name: Smyth

*Full name: Alice Smyth

*Preferred user ID: asmyth

First name: Alice

Initials:

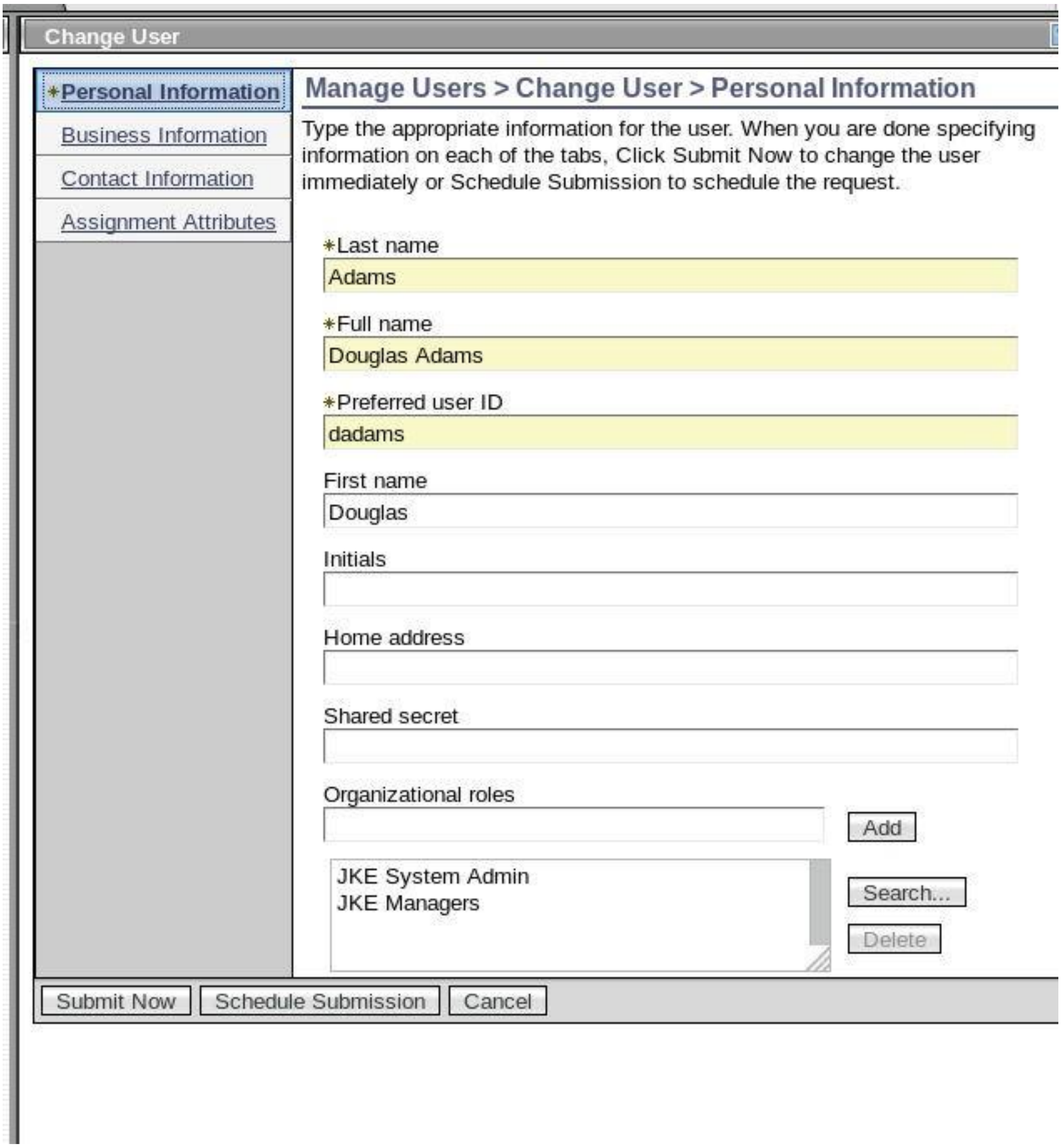
Home address:

Shared secret:

Organizational roles:

JKE System Admin
Asset Handling And Disposition
Booking and Ledgers
ITIM Administrators

6. Repeat steps 3-5 for user **Douglas Adams**.



Change User

Manage Users > Change User > Personal Information

Type the appropriate information for the user. When you are done specifying information on each of the tabs, Click Submit Now to change the user immediately or Schedule Submission to schedule the request.

*Last name: Adams

*Full name: Douglas Adams

*Preferred user ID: dadams

First name: Douglas

Initials:

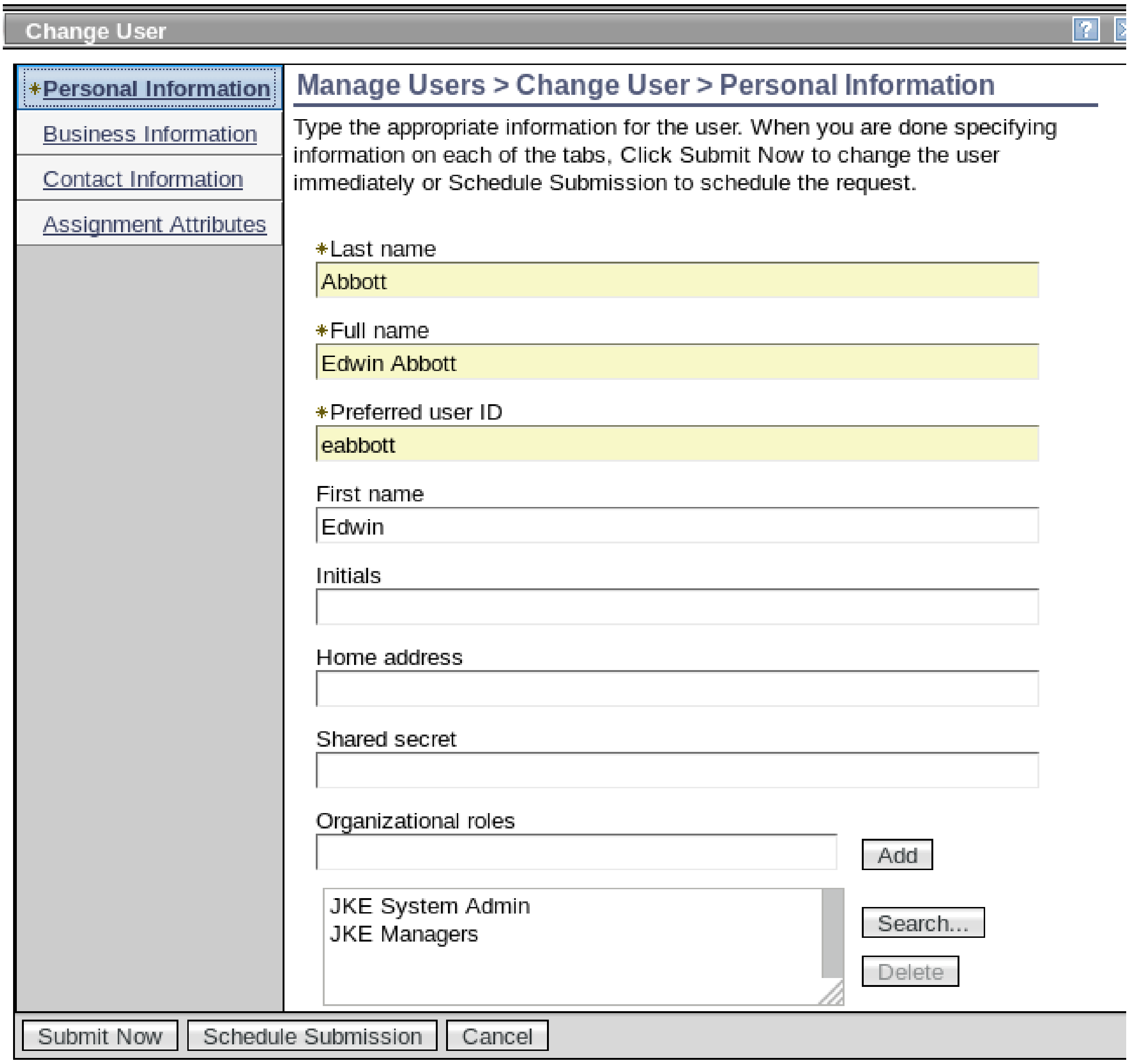
Home address:

Shared secret:

Organizational roles:

JKE System Admin
JKE Managers

7. Repeat steps 3-5 for user **Edwin Abbott**.



Manage Users > Change User > Personal Information

Type the appropriate information for the user. When you are done specifying information on each of the tabs, Click Submit Now to change the user immediately or Schedule Submission to schedule the request.

*Last name: Abbott

*Full name: Edwin Abbott

*Preferred user ID: eabbott

First name: Edwin

Initials:

Home address:

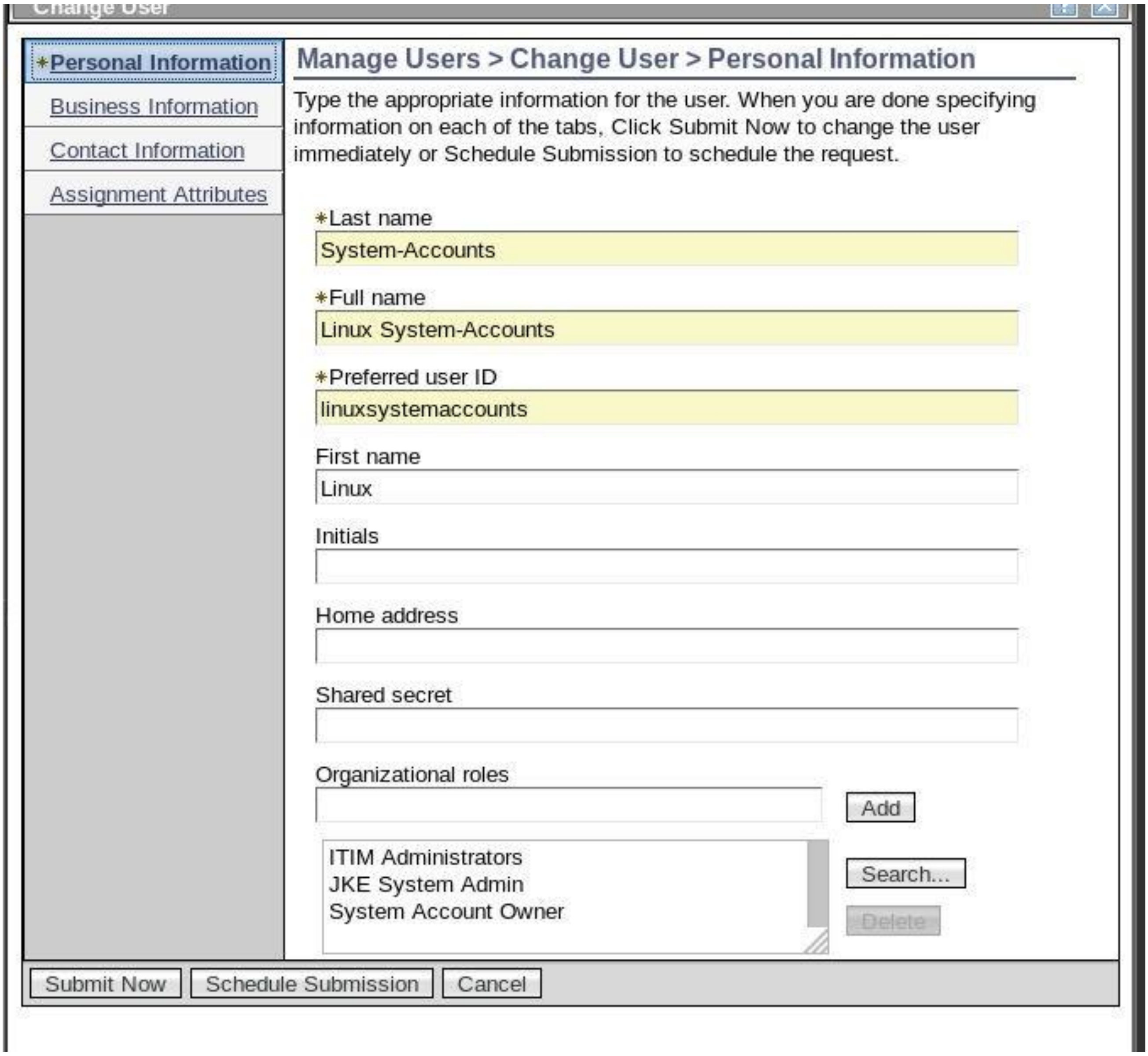
Shared secret:

Organizational roles:

JKE System Admin
JKE Managers

Task 2: Assign System Accounts Owner Role

1. Navigate to **Home** $\rightarrow$ **Manage Users**.
2. Search for and select user **Linux System-Accounts** $\rightarrow$ **Personal Information** tab.



Manage Users > Change User > Personal Information

Type the appropriate information for the user. When you are done specifying information on each of the tabs, Click Submit Now to change the user immediately or Schedule Submission to schedule the request.

*Last name: System-Accounts

*Full name: Linux System-Accounts

*Preferred user ID: linuxsystemaccounts

First name: Linux

Initials:

Home address:

Shared secret:

Organizational roles:

ITIM Administrators
JKE System Admin
System Account Owner

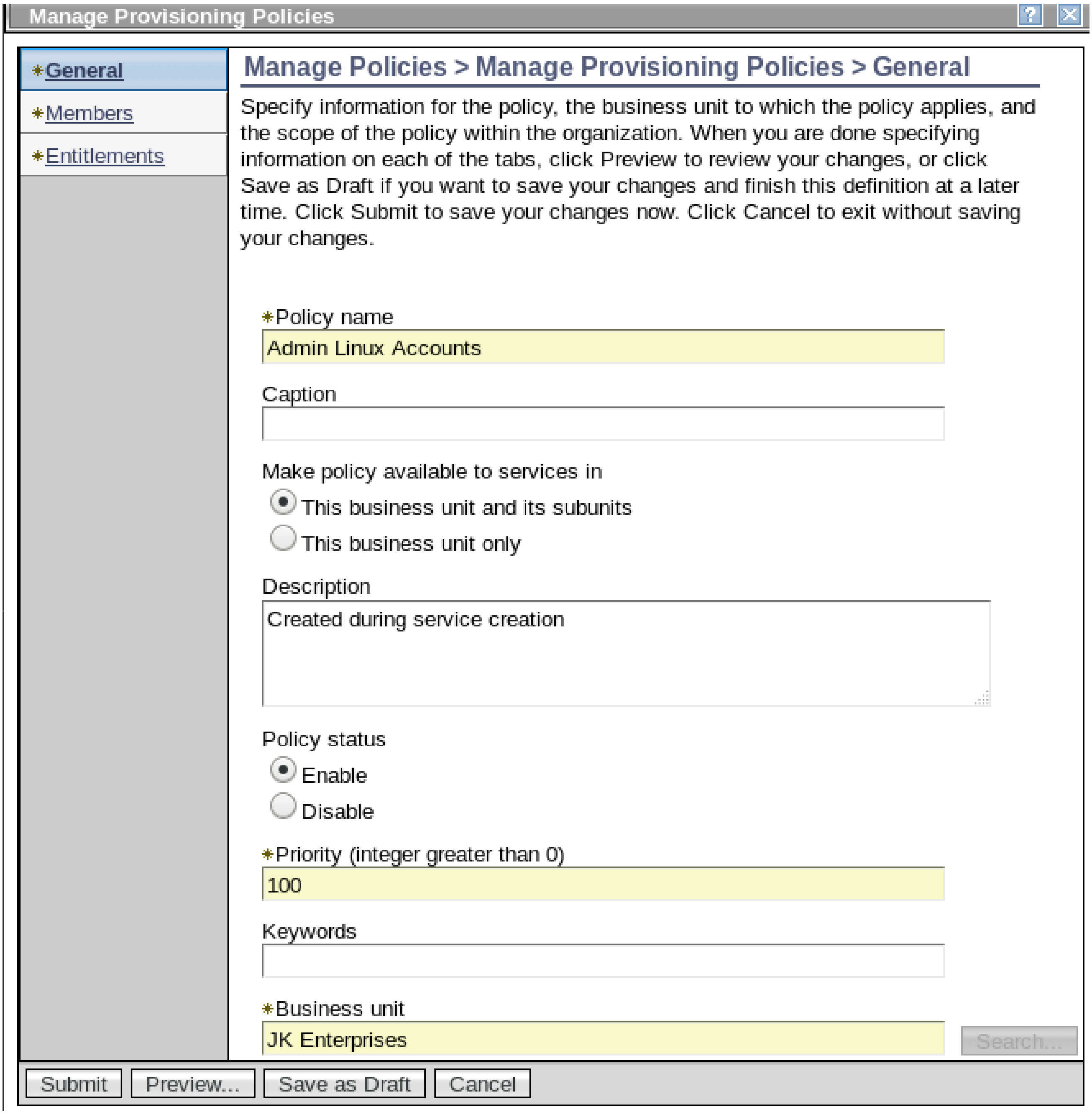
3. Add the **System Accounts Owner** organizational role to Linux System-Accounts.
4. Click **Submit Now** $\rightarrow$ **Close**.

Exercise 7.2 – Creating a Provisioning Policy

Objective: Enable automatic Linux account creation for users in the JKE System Admin role.

1. Navigate to **Home** $\rightarrow$ **Manage Policies** $\rightarrow$ **Manage Provisioning Policies**.
2. Open the **Default Provisioning Policy for Linux Service**.
3. Modify the policy details as follows:
   - Set **Policy Name** to **Admin Linux Accounts**.

- Set **Status** to **Enabled**.
- Set **Priority** to **100**.
- Set **Members** to the organizational role **JKE System Admin**.



Manage Policies > Manage Provisioning Policies > General

Specify information for the policy, the business unit to which the policy applies, and the scope of the policy within the organization. When you are done specifying information on each of the tabs, click Preview to review your changes, or click Save as Draft if you want to save your changes and finish this definition at a later time. Click Submit to save your changes now. Click Cancel to exit without saving your changes.

*Policy name: Admin Linux Accounts

Caption:

Make policy available to services in
● This business unit and its subunits
○ This business unit only

Description: Created during service creation

Policy status
● Enable
○ Disable

*Priority (integer greater than 0): 100

Keywords:

*Business unit: JK Enterprises

4. Navigate to **Entitlements Configuration**.
5. Select **Linux Service** $\rightarrow$ **Change**.
6. Set **Provisioning Options** to **Automatic**.
7. Set **Target Type** to **Specific Service**.
8. Set **Service Name** to **Linux Service**.

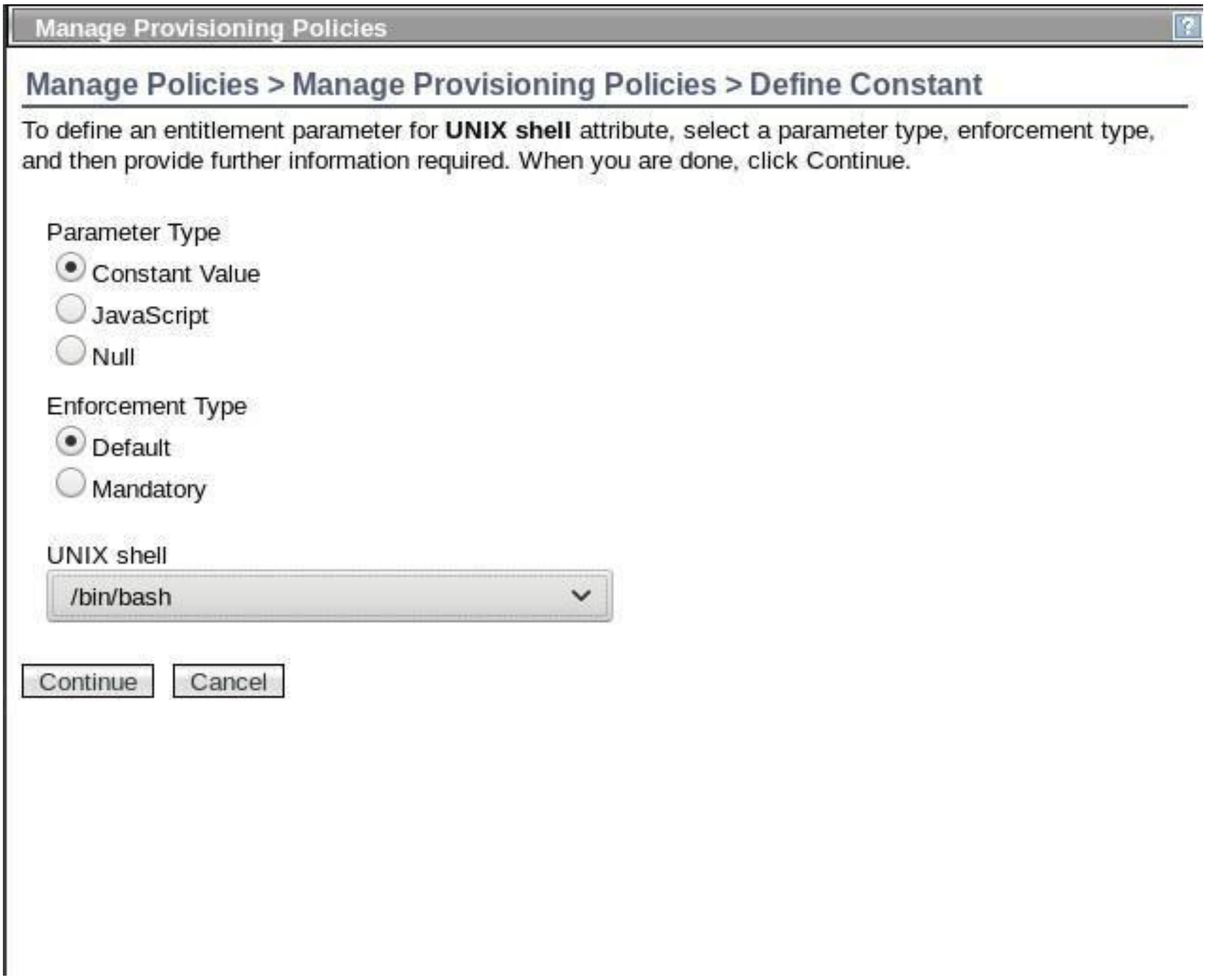
9. Leave **Workflow** field empty.

10. Click **Preview & Submit**.

11. On the Preview screen, choose to **enforce entire policy**.

12. Confirm the expected outcome of **4 new accounts** (Alice, Douglas, Edwin, Erica).

13. **Submit** and **enforce** the policy.



Manage Provisioning Policies

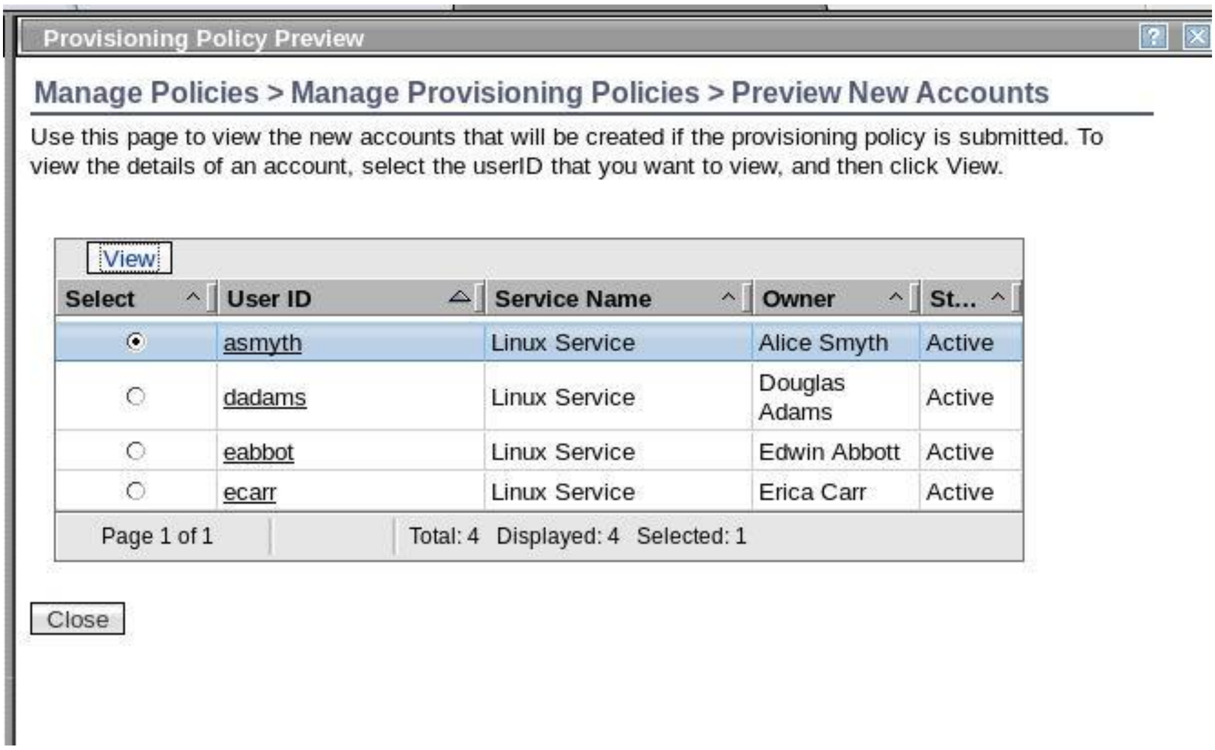
Manage Policies > Manage Provisioning Policies > Define Constant

To define an entitlement parameter for **UNIX shell** attribute, select a parameter type, enforcement type, and then provide further information required. When you are done, click Continue.

Parameter Type
● Constant Value
○ JavaScript
○ Null

Enforcement Type
● Default
○ Mandatory

UNIX shell
/bin/bash



Provisioning Policy Preview

Manage Policies > Manage Provisioning Policies > Preview New Accounts

Use this page to view the new accounts that will be created if the provisioning policy is submitted. To view the details of an account, select the userID that you want to view, and then click View.

Select	User ID	Service Name	Owner	St...
●	asmyth	Linux Service	Alice Smyth	Active
○	dadams	Linux Service	Douglas Adams	Active
○	eabbot	Linux Service	Edwin Abbott	Active
○	ecarr	Linux Service	Erica Carr	Active

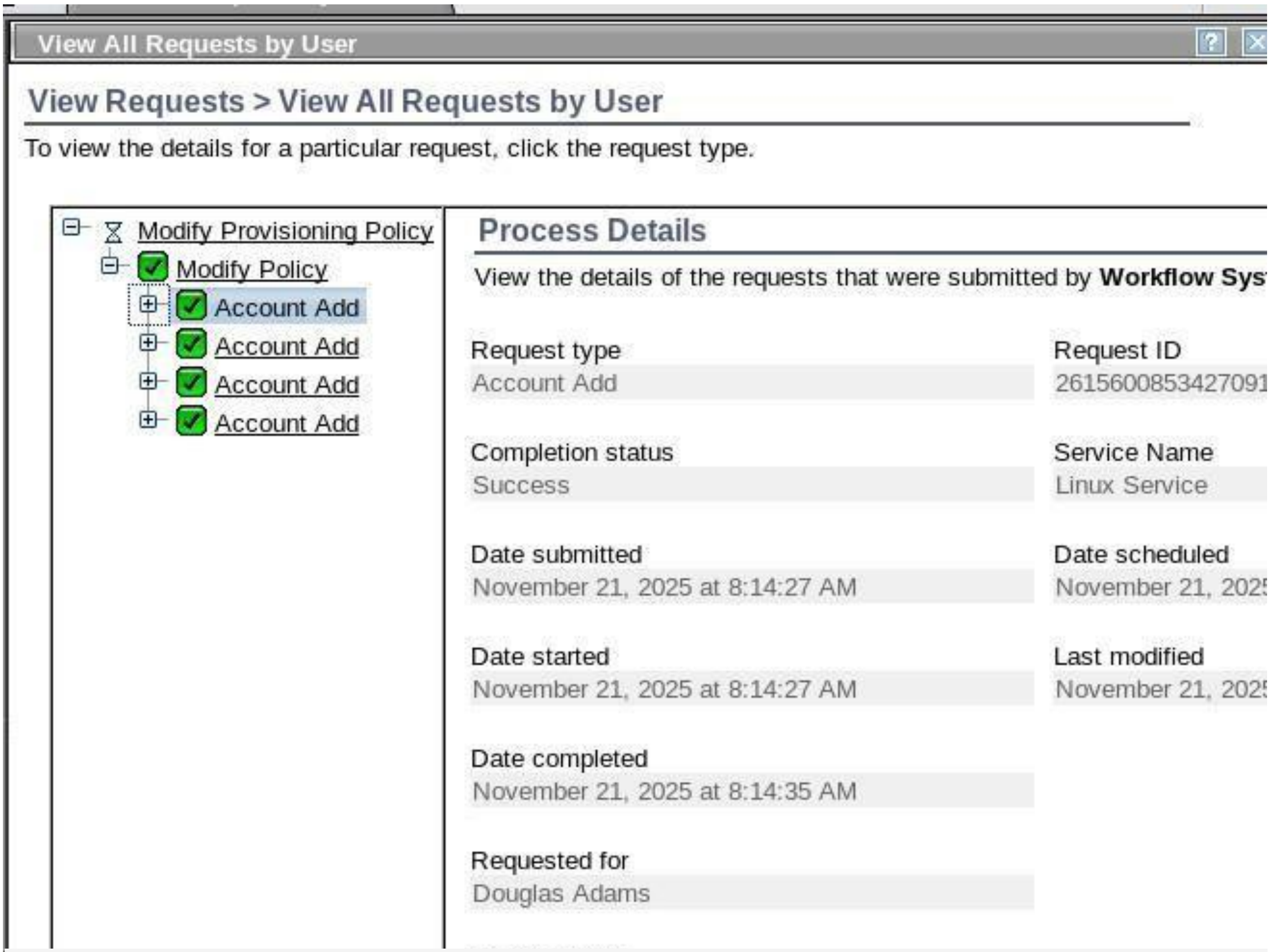
Page 1 of 1 Total: 4 Displayed: 4 Selected: 1

Exercise 7.3 – Verifying Linux Account

Provisioning Objective: Review requests and

confirm accounts on Linux.

1. Navigate to **Home** $\rightarrow$ **View Requests** $\rightarrow$ **View All Requests by User**.
2. Open the **Modify Provisioning Policy** request associated with the policy enforcement.
3. Confirm that the request details show the successful creation of **4 accounts**.
4. *Implied:* Navigate to the accounts of Alice, Douglas, Edwin, and Erica and verify the existence of their new Linux accounts.



View All Requests by User

View Requests > View All Requests by User

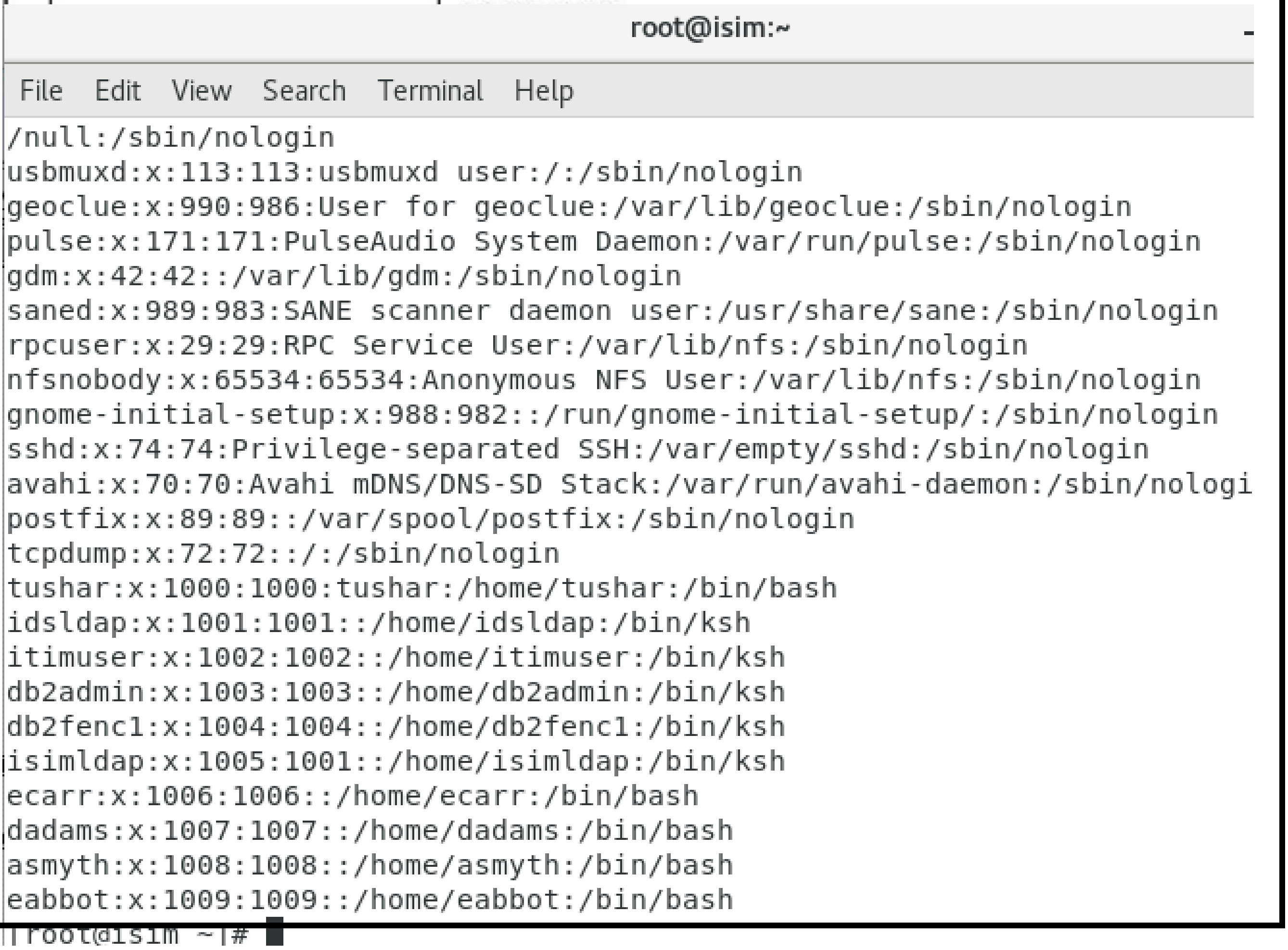
To view the details for a particular request, click the request type.

- Modify Provisioning Policy
  - Modify Policy
    - Account Add
    - Account Add
    - Account Add
    - Account Add

Process Details

View the details of the requests that were submitted by **Workflow Sys**

Request type Account Add	Request ID 261560085342709l
Completion status Success	Service Name Linux Service
Date submitted November 21, 2025 at 8:14:27 AM	Date scheduled November 21, 202
Date started November 21, 2025 at 8:14:27 AM	Last modified November 21, 202
Date completed November 21, 2025 at 8:14:35 AM	
Requested for Douglas Adams	

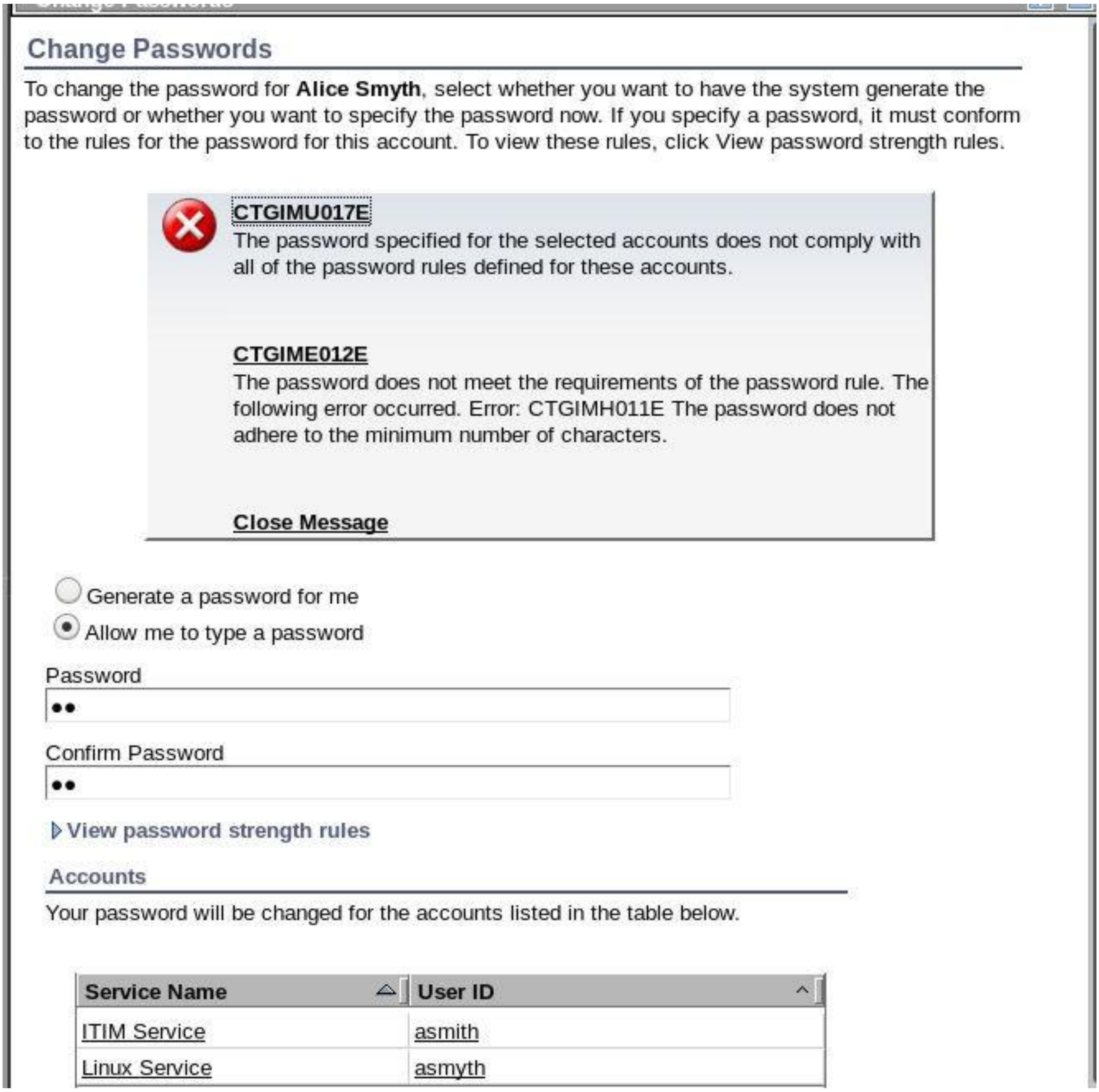


```
/null:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:990:986:User for geoclue:/var/lib/geoclue:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
saned:x:989:983:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:988:982::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologi
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
tushar:x:1000:1000:tushar:/home/tushar:/bin/bash
idsldap:x:1001:1001::/home/idsldap:/bin/ksh
itimuser:x:1002:1002::/home/itimuser:/bin/ksh
db2admin:x:1003:1003::/home/db2admin:/bin/ksh
db2fenc1:x:1004:1004::/home/db2fenc1:/bin/ksh
isimldap:x:1005:1001::/home/isimldap:/bin/ksh
ecarr:x:1006:1006::/home/ecarr:/bin/bash
dadams:x:1007:1007::/home/dadams:/bin/bash
asmyth:x:1008:1008::/home/asmyth:/bin/bash
eabbot:x:1009:1009::/home/eabbot:/bin/bash
[root@isim ~]#
```

Exercise 7.4 – Verifying Password Policy

Objective: Confirm password restrictions for the Linux Service.

1. Navigate to **Home** $\rightarrow$ **Manage Users** $\rightarrow$ **Alice Smyth**.
2. Select the **Change Passwords** tab/action.
3. Enter a short password, such as aa, and click **Submit**.
4. Observe the resulting **password violation message** (e.g., "Password does not meet minimum length requirements").



Change Passwords

To change the password for **Alice Smyth**, select whether you want to have the system generate the password or whether you want to specify the password now. If you specify a password, it must conform to the rules for the password for this account. To view these rules, click View password strength rules.

CTGIMU017E
The password specified for the selected accounts does not comply with all of the password rules defined for these accounts.

CTGIME012E
The password does not meet the requirements of the password rule. The following error occurred. Error: CTGIMH011E The password does not adhere to the minimum number of characters.

Close Message

○ Generate a password for me
● Allow me to type a password

Password
••

Confirm Password
••

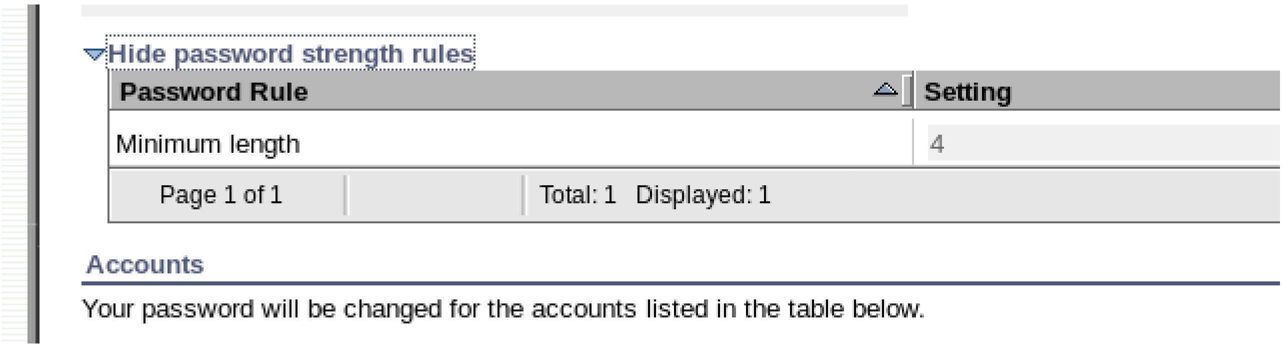
View password strength rules

Accounts

Your password will be changed for the accounts listed in the table below.

Service Name	User ID
ITIM Service	asmith
Linux Service	asmyth

5. Check the configured password strength rules for the Linux service profile.



▽Hide password strength rules

Password Rule	Setting
Minimum length	4

Page 1 of 1 Total: 1 Displayed: 1

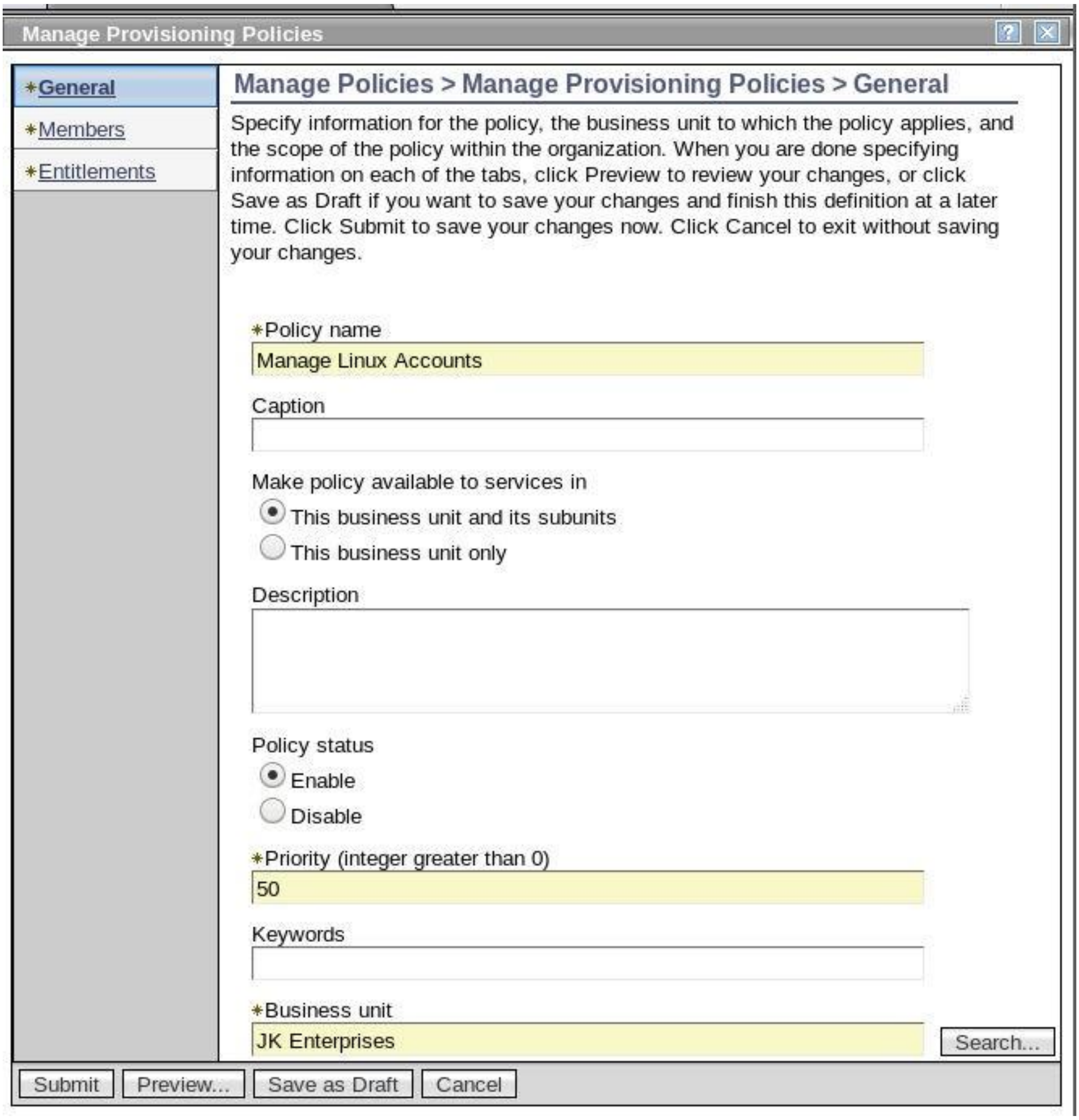
Accounts

Your password will be changed for the accounts listed in the table below.

Exercise 7.5 – Creating a Provisioning Policy for JKE Managers

Objective: Give Linux accounts to users in the JKE Managers role and introduce an attribute conflict.

1. Create a new provisioning policy.
2. Set the policy details as follows:
   - Set **Policy Name** to **Manager Linux Accounts**.
   - Set **Status** to **Enabled**.
   - Set **Priority** to **50**.
   - Set **Members** to the organizational role **JKE Managers**.



Manage Policies > Manage Provisioning Policies > General

Specify information for the policy, the business unit to which the policy applies, and the scope of the policy within the organization. When you are done specifying information on each of the tabs, click Preview to review your changes, or click Save as Draft if you want to save your changes and finish this definition at a later time. Click Submit to save your changes now. Click Cancel to exit without saving your changes.

*Policy name: Manage Linux Accounts

Caption:

Make policy available to services in
● This business unit and its subunits
○ This business unit only

Description:

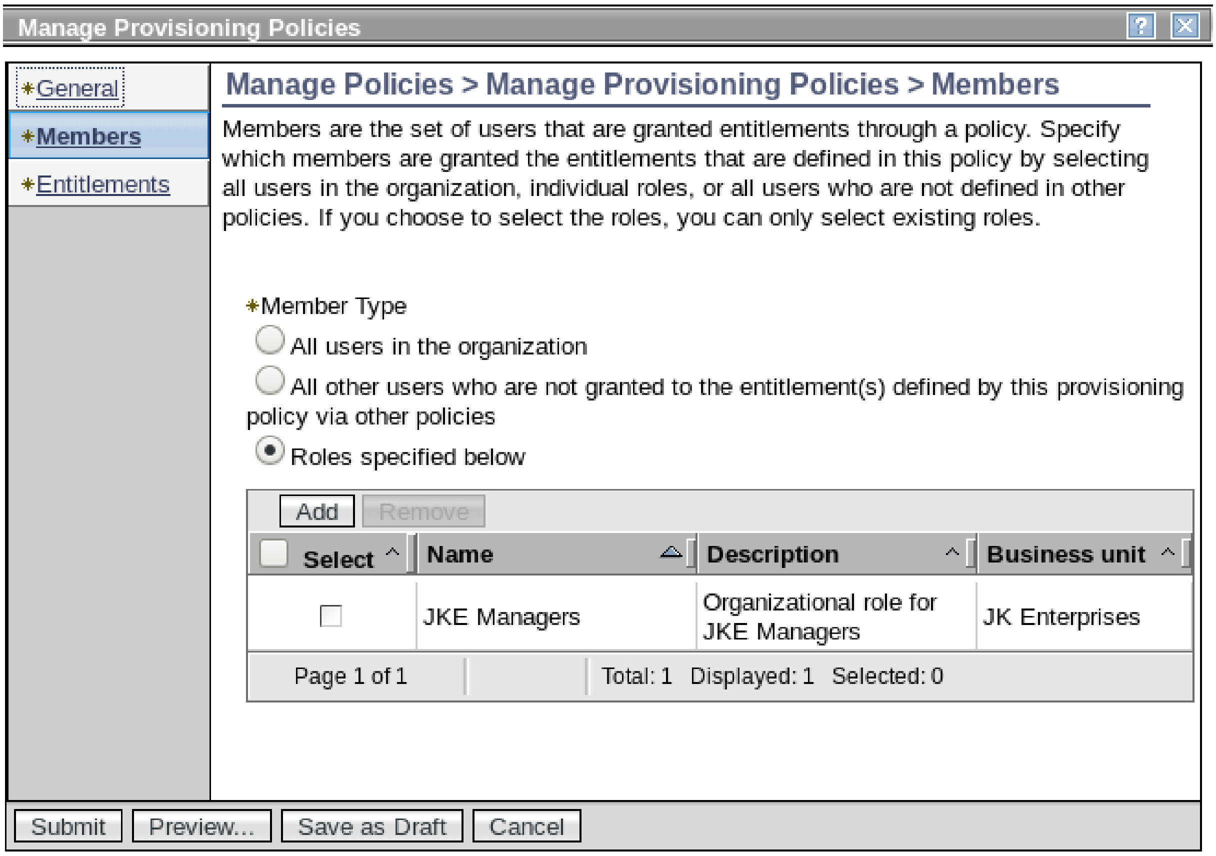
Policy status
● Enable
○ Disable

*Priority (integer greater than 0): 50

Keywords:

*Business unit: JK Enterprises

3. Navigate to **Entitlements Configuration** $\rightarrow$ **Linux Service** $\rightarrow$ **Parameters**.



Manage Provisioning Policies

Manage Policies > Manage Provisioning Policies > Members

Members are the set of users that are granted entitlements through a policy. Specify which members are granted the entitlements that are defined in this policy by selecting all users in the organization, individual roles, or all users who are not defined in other policies. If you choose to select the roles, you can only select existing roles.

*Member Type

○ All users in the organization

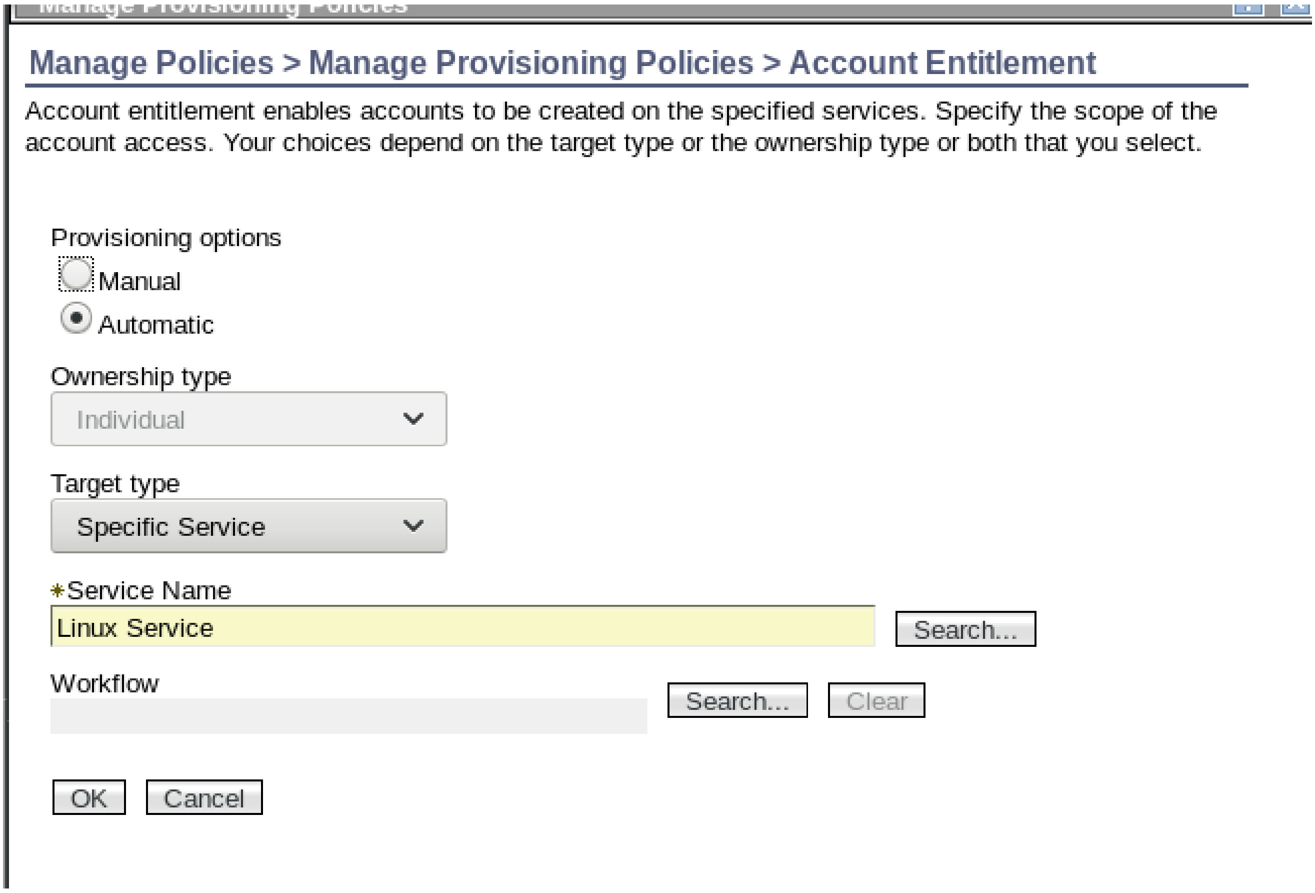
○ All other users who are not granted to the entitlement(s) defined by this provisioning policy via other policies

● Roles specified below

□ Select	Name	Description	Business unit
□	JKE Managers	Organizational role for JKE Managers	JK Enterprises

Page 1 of 1 Total: 1 Displayed: 1 Selected: 0

4. Add an entitlement parameter:
   - Set **Attribute** to **Shell**.
   - Set **Enforcement Type** to **Mandatory**.
   - Set **Value** to **/bin/ksh**.



Manage Provisioning Policies

Manage Policies > Manage Provisioning Policies > Account Entitlement

Account entitlement enables accounts to be created on the specified services. Specify the scope of the account access. Your choices depend on the target type or the ownership type or both that you select.

Provisioning options

○ Manual

● Automatic

Ownership type: Individual

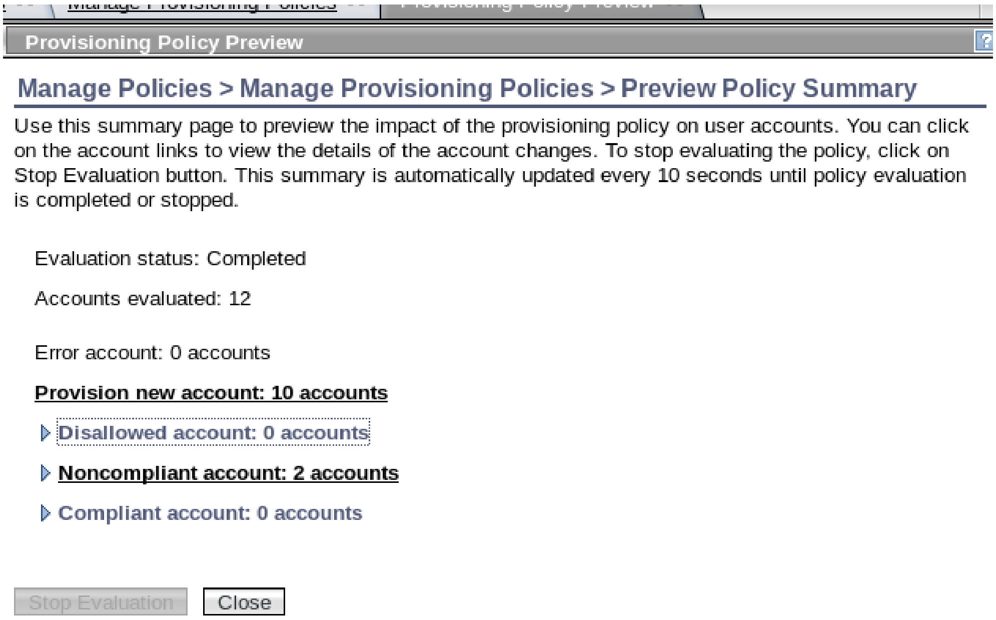
Target type: Specific Service

*Service Name: Linux Service

Workflow:

5. Submit and enforce the policy.

6. **Expected Outcome:** New accounts are provisioned for JKE Managers. Users Douglas and Edwin (who are in both roles) will be flagged as **non-compliant** because their existing Linux account shell does not match the mandatory /bin/ksh value, and the Manager policy has higher precedence (Priority 50 is lower than 100).



Provisioning Policy Preview

Manage Policies > Manage Provisioning Policies > Preview Policy Summary

Use this summary page to preview the impact of the provisioning policy on user accounts. You can click on the account links to view the details of the account changes. To stop evaluating the policy, click on Stop Evaluation button. This summary is automatically updated every 10 seconds until policy evaluation is completed or stopped.

Evaluation status: Completed

Accounts evaluated: 12

Error account: 0 accounts

Provision new account: 10 accounts

Disallowed account: 0 accounts

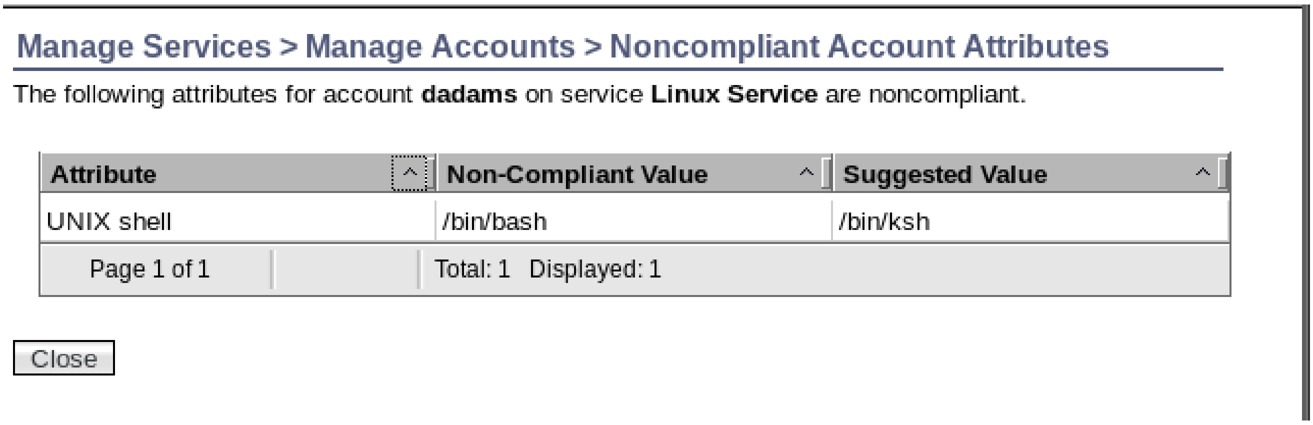
Noncompliant account: 2 accounts

Compliant account: 0 accounts

Exercise 7.6 – Verifying Policy Priority

Objective: Confirm that the Manager policy (Priority 50) overrides the Admin policy (Priority 100).

1. Navigate to **Manage Users** $\rightarrow$ **Douglas Adams** $\rightarrow$ **Accounts** tab.
2. Open the Linux account details.
3. Observe the **Warning: Shell non-compliant** message, confirming that the Manager policy is dictating the correct value.
4. Note that the account is not automatically corrected because the policy's enforcement mode is set to **Mark** (not Correct).



Manage Services > Manage Accounts > Noncompliant Account Attributes

The following attributes for account **dadams** on service **Linux Service** are noncompliant.

Attribute	Non-Compliant Value	Suggested Value
UNIX shell	/bin/bash	/bin/ksh

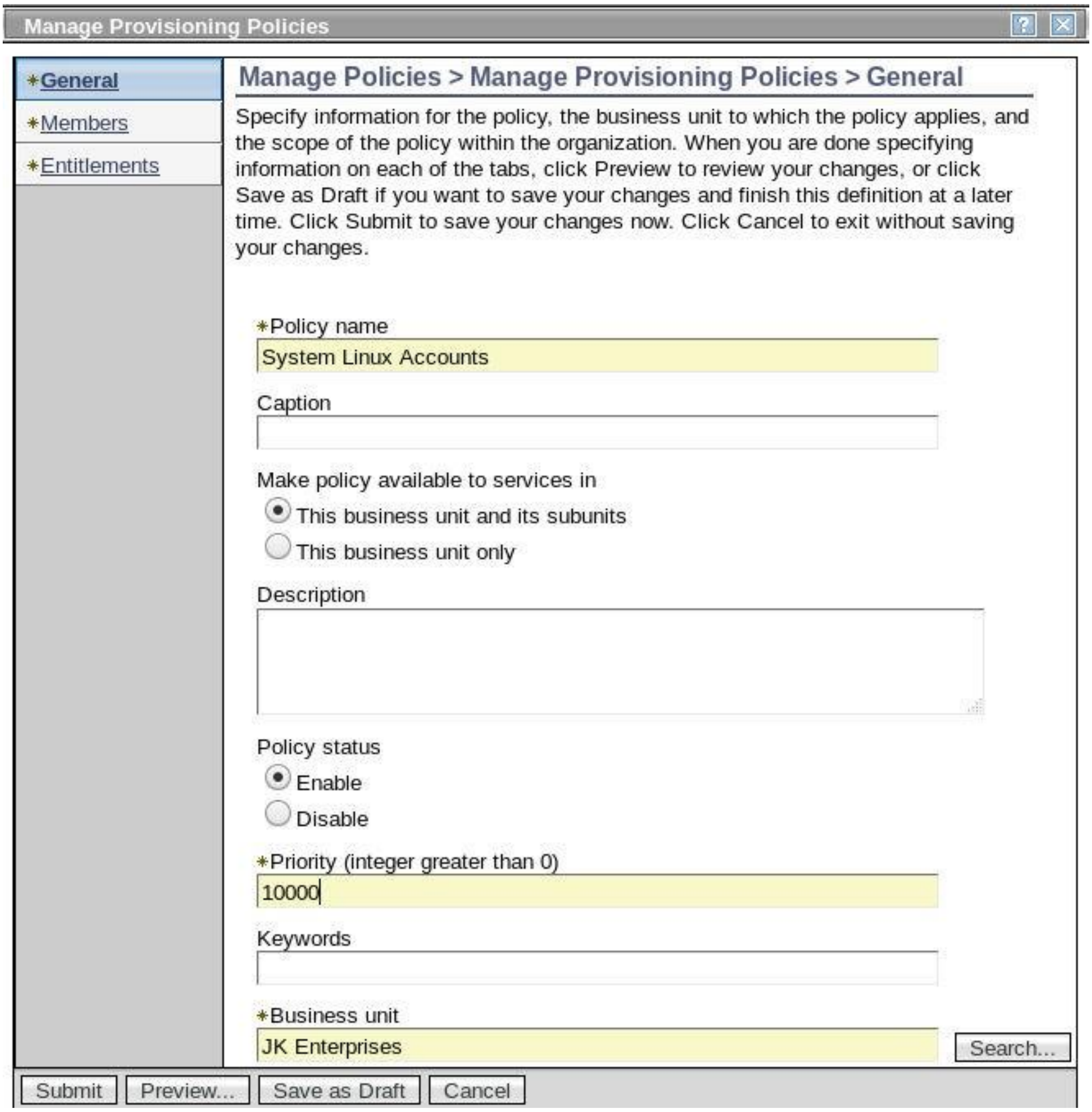
Page 1 of 1   Total: 1   Displayed: 1

Exercise 7.7 – Provisioning Policy for System Accounts

Objective: Ensure the Linux System-Accounts user owns system accounts.

Task 1: Policy Setup

1. Create a new provisioning policy.
2. Set the policy details as follows:
   - Set **Policy Name** to **System Linux Accounts**.
   - Set **Priority** to **10000**.
   - Set **Members** to the organizational role **System Account Owner**.
   - Set **Ownership Type** to **System**.
   - Set **Provisioning** to **Manual**.



Manage Policies > Manage Provisioning Policies > General

Specify information for the policy, the business unit to which the policy applies, and the scope of the policy within the organization. When you are done specifying information on each of the tabs, click Preview to review your changes, or click Save as Draft if you want to save your changes and finish this definition at a later time. Click Submit to save your changes now. Click Cancel to exit without saving your changes.

*Policy name: System Linux Accounts

Caption:

Make policy available to services in
● This business unit and its subunits
○ This business unit only

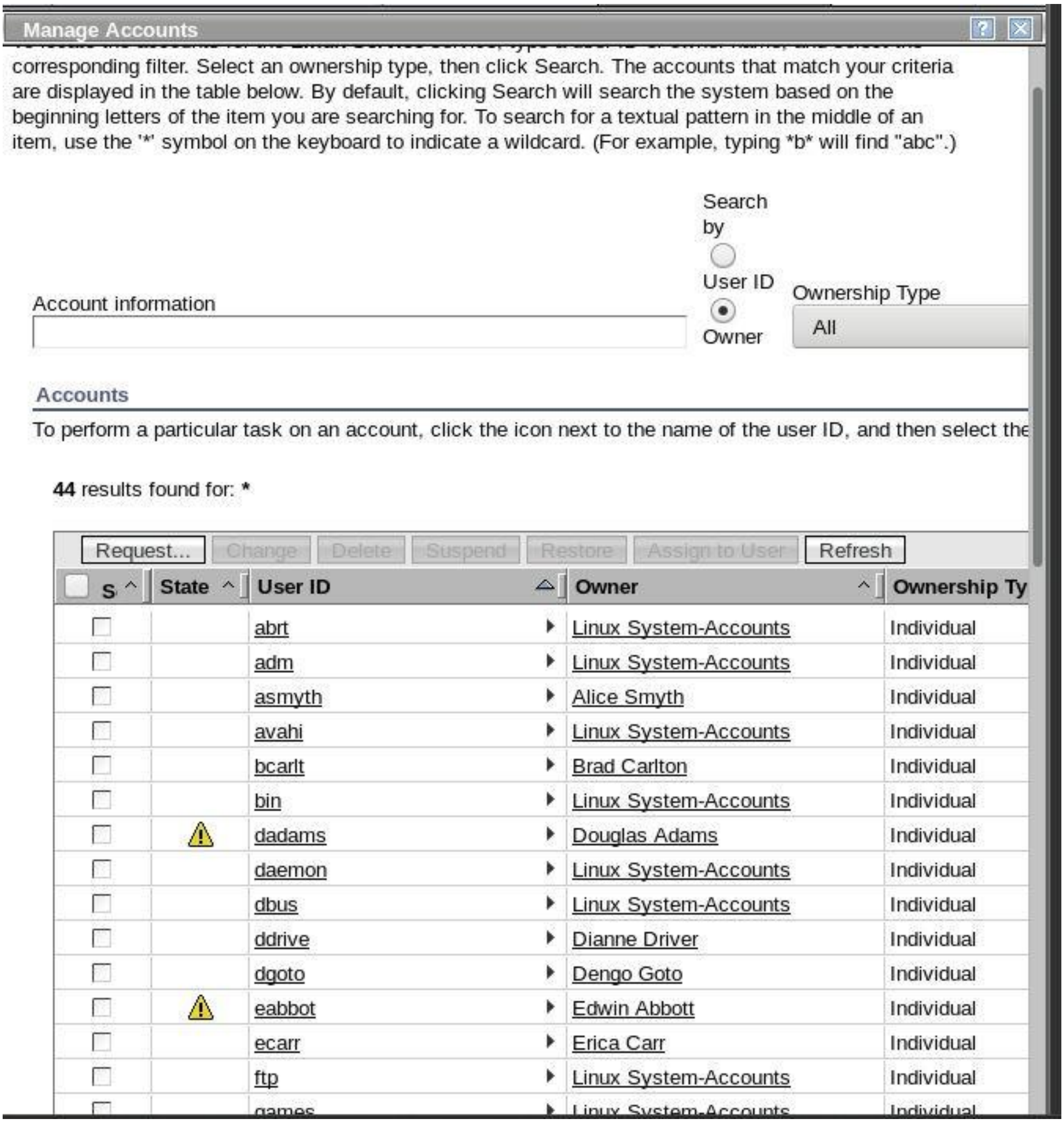
Description:

Policy status
● Enable
○ Disable

*Priority (integer greater than 0): 10000

Keywords:

*Business unit: JK Enterprises



Manage Accounts

corresponding filter. Select an ownership type, then click Search. The accounts that match your criteria are displayed in the table below. By default, clicking Search will search the system based on the beginning letters of the item you are searching for. To search for a textual pattern in the middle of an item, use the '*' symbol on the keyboard to indicate a wildcard. (For example, typing *b* will find "abc".)

Account information:

Search by: ○ User ID ● Owner

Ownership Type: All

Accounts

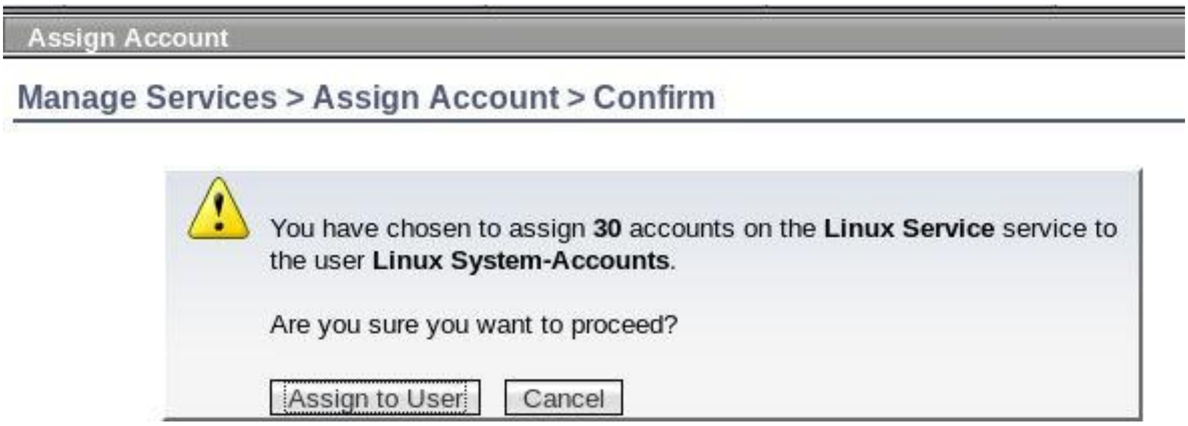
To perform a particular task on an account, click the icon next to the name of the user ID, and then select the

44 results found for: *

□	S	State	User ID	Owner	Ownership Ty
□			abrt	Linux System-Accounts	Individual
□			adm	Linux System-Accounts	Individual
□			asmyth	Alice Smyth	Individual
□			avahi	Linux System-Accounts	Individual
□			bcarlt	Brad Carlton	Individual
□			bin	Linux System-Accounts	Individual
□		⚠	dadams	Douglas Adams	Individual
□			daemon	Linux System-Accounts	Individual
□			dbus	Linux System-Accounts	Individual
□			ddrive	Dianne Driver	Individual
□			dgoto	Dengo Goto	Individual
□		⚠	eabbot	Edwin Abbott	Individual
□			ecarr	Erica Carr	Individual
□			ftp	Linux System-Accounts	Individual
□			games	Linux System-Accounts	Individual

Task 2: Change Ownership

1. Navigate to the service containing the system accounts (e.g., Linux Service).
2. Filter the accounts to select those that should be system-owned.



Manage Services > Assign Account > Confirm

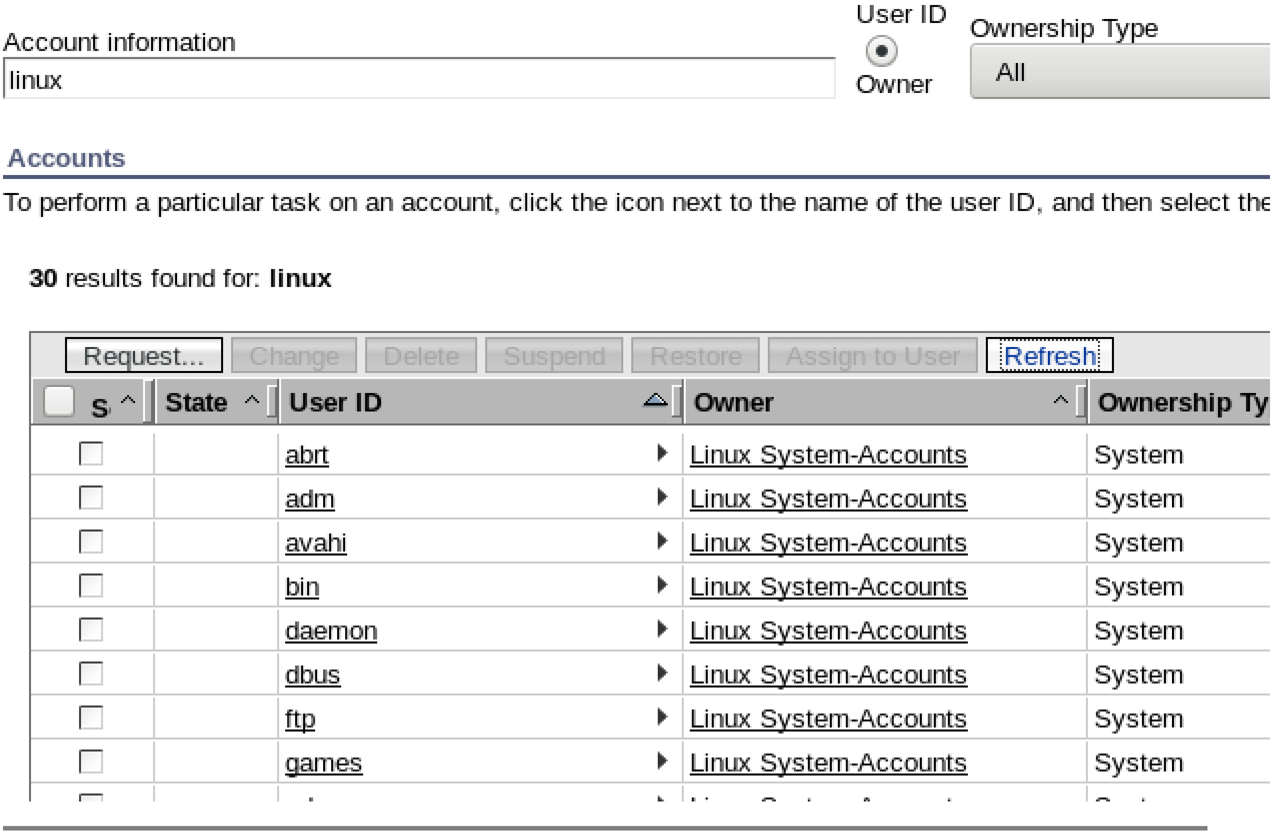
You have chosen to assign **30** accounts on the **Linux Service** service to the user **Linux System-Accounts**.

Are you sure you want to proceed?

3. Select the accounts $\rightarrow$ **Assign to User**.

4. Select the user **Linux System-Accounts**.

5. Confirm that the selected accounts now display **System ownership**.



Account information: linux

User ID ○ Owner ●

Ownership Type: All

Accounts

To perform a particular task on an account, click the icon next to the name of the user ID, and then select the

30 results found for: **linux**

S	State	User ID	Owner	Ownership Ty
□		abrt	Linux System-Accounts	System
□		adm	Linux System-Accounts	System
□		avahi	Linux System-Accounts	System
□		bin	Linux System-Accounts	System
□		daemon	Linux System-Accounts	System
□		dbus	Linux System-Accounts	System
□		ftp	Linux System-Accounts	System
□		games	Linux System-Accounts	System

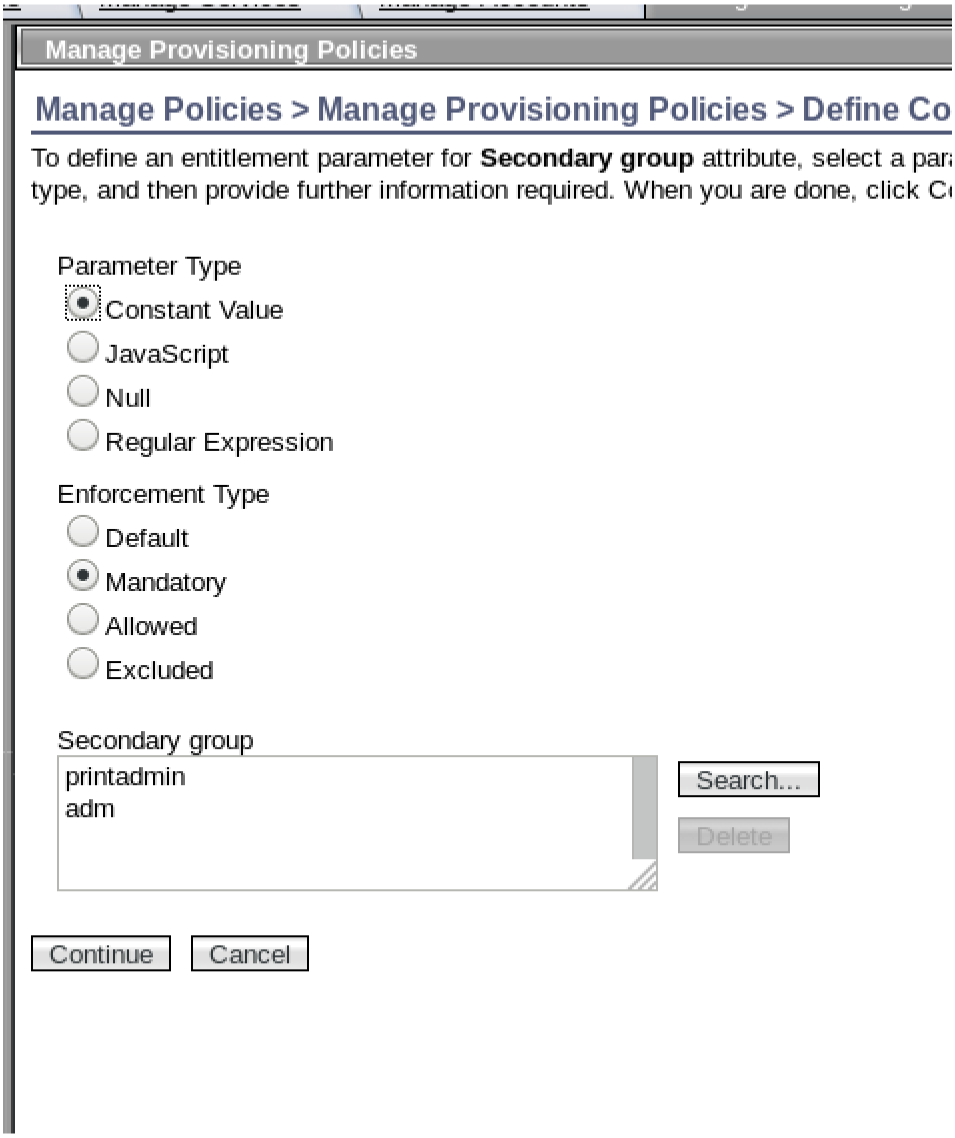
Exercise 7.8 – Modifying the Default Join Directive for an Attribute

Objective: Understand attribute join behavior and how conflicts are resolved (Union vs. Intersection).

PART 1 & 2 – Modify Existing Provisioning Policies to Create Attribute Conflicts

1. **Edit Admin Linux Accounts Policy:**
    - Go to **Entitlements** $\rightarrow$ **Linux Service** $\rightarrow$ **Parameters**.

- Create **Parameter 1** (Mandatory groups):
  - Attribute: **Secondary group** (erposixsecondgroup).
  - Enforcement Type: **Mandatory**.
  - Groups: adm, printadmin.



Manage Provisioning Policies

Manage Policies > Manage Provisioning Policies > Define Co

To define an entitlement parameter for **Secondary group** attribute, select a par
type, and then provide further information required. When you are done, click C

Parameter Type

● Constant Value
○ JavaScript
○ Null
○ Regular Expression

Enforcement Type

○ Default
● Mandatory
○ Allowed
○ Excluded

Secondary group

printadmin
adm

- Create **Parameter 2** (Allowed groups):
  - Attribute: **Secondary group**.
  - Enforcement Type: **Allowed**.
  - Groups: dialout, games, video.
- Submit and enforce the policy.

2. **Edit Manager Linux Accounts Policy:**

- Repeat the steps above, but use different groups:

- Parameter 1 (Mandatory): printadmin.
- Parameter 2 (Allowed): dialout, video (do NOT include games).

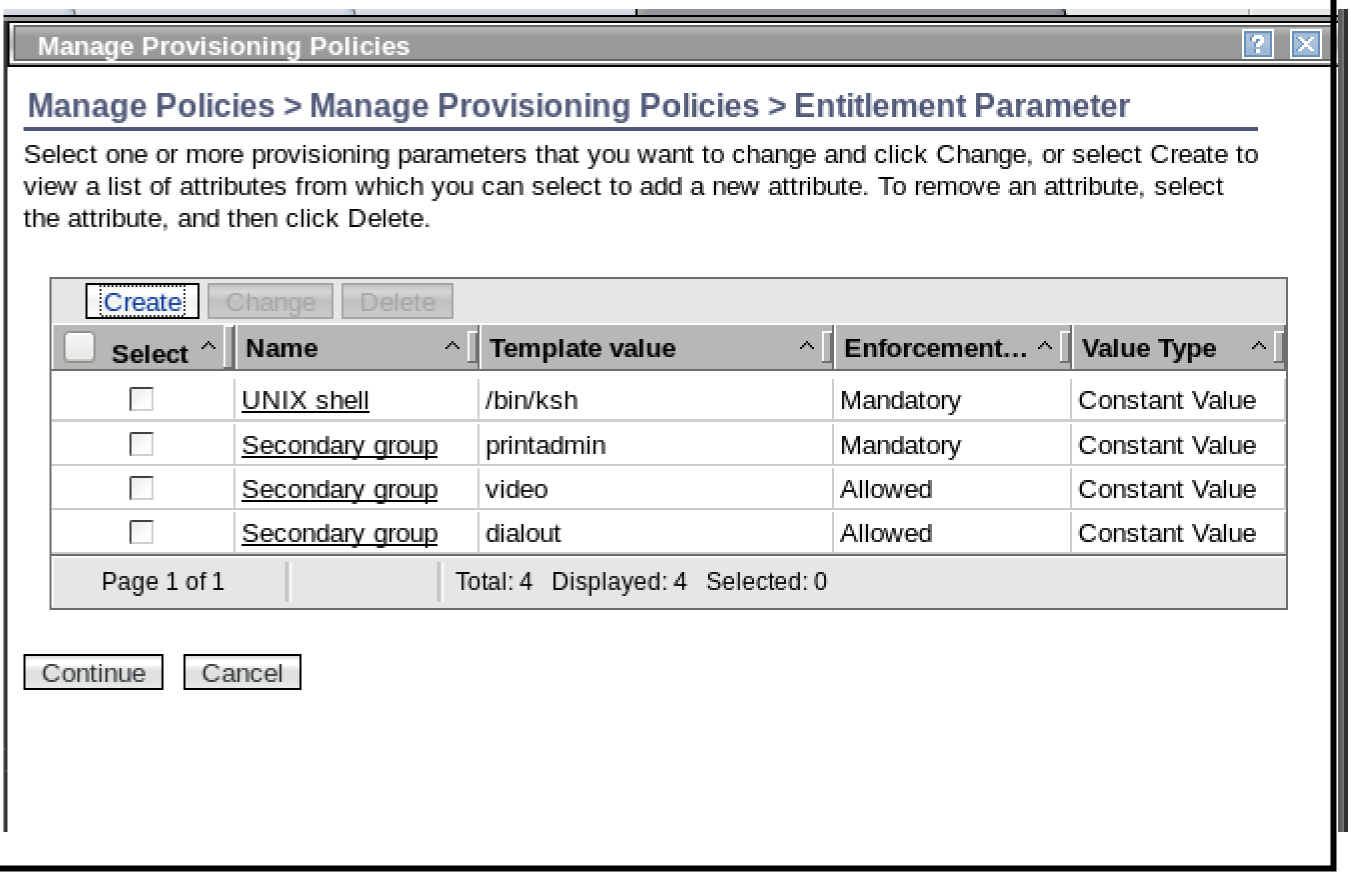
- Submit and enforce the policy.

3. Wait for both requests to complete via **Home** $\rightarrow$

View Requests. PART 2 – Create a New User to Observe Join

Behavior (UNION)

1. Navigate to **Manage Users** $\rightarrow$ **Create Person**.
2. Create user **Uma Join** (Preferred User ID: ujoin).
3. Assign the Organizational Role **JKE System Admin** and set the Title to **Manager** (to ensure both policies apply).
4. Submit the user.
5. On the Linux terminal, check the groups assigned to ujoin.
   - **Expected Output (UNION - Default):** The user has all mandatory + allowed groups combined from both policies: printadmin, adm, dialout, games, video.



Manage Policies > Manage Provisioning Policies > Entitlement Parameter

Select one or more provisioning parameters that you want to change and click Change, or select Create to view a list of attributes from which you can select to add a new attribute. To remove an attribute, select the attribute, and then click Delete.

□ Select	Name	Template value	Enforcement...	Value Type
□	UNIX shell	/bin/ksh	Mandatory	Constant Value
□	Secondary group	printadmin	Mandatory	Constant Value
□	Secondary group	video	Allowed	Constant Value
□	Secondary group	dialout	Allowed	Constant Value

Page 1 of 1 Total: 4 Displayed: 4 Selected: 0

PART 3 & 4 – Change Join Directive to INTERSECTION

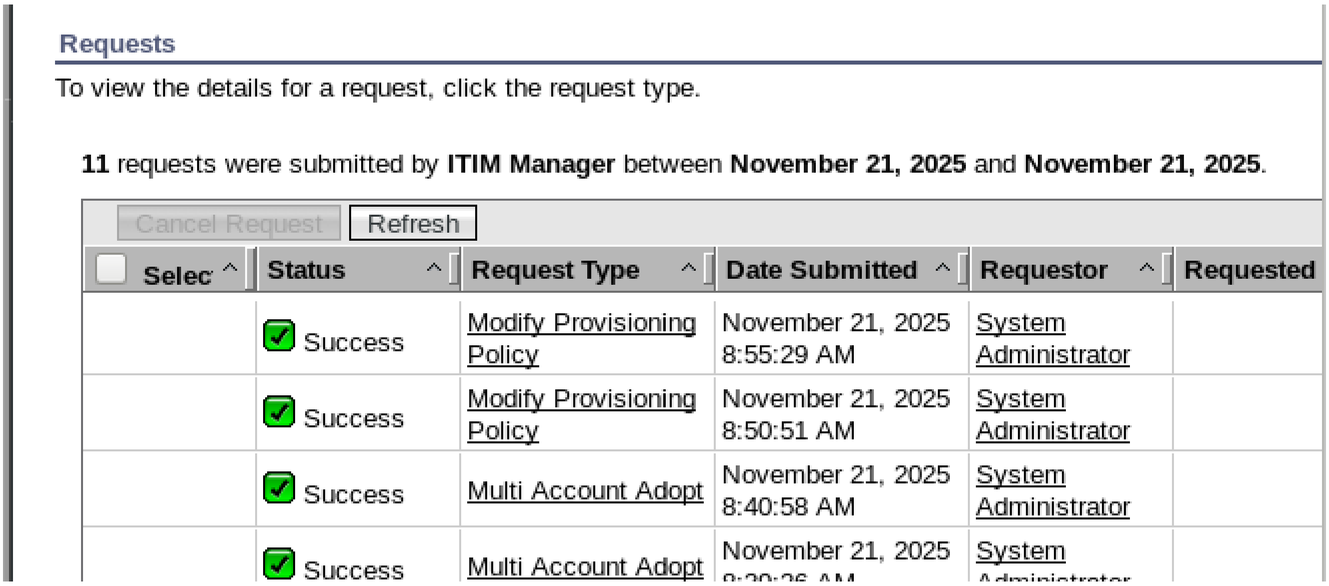
1. Navigate to **Configure System** $\rightarrow$ **Configure Policy Join Behaviors**.
2. Open the configuration using **Java Webstart**.
3. Select **Service Type**: **PosixLinuxProfile**.

4. From the attribute list, select: erposixsecondgroup (**Secondary group**).

5. Change **Join Type** to **Intersection**.

6. Click **Save** and close the window.

7. **Restart ISIM Server** (required to apply the change).



Requests

To view the details for a request, click the request type.

11 requests were submitted by **ITIM Manager** between **November 21, 2025** and **November 21, 2025**.

□ Selec	Status	Request Type	Date Submitted	Requestor	Requested
	✓ Success	Modify Provisioning Policy	November 21, 2025 8:55:29 AM	System Administrator	
	✓ Success	Modify Provisioning Policy	November 21, 2025 8:50:51 AM	System Administrator	
	✓ Success	Multi Account Adopt	November 21, 2025 8:40:58 AM	System Administrator	
	✓ Success	Multi Account Adopt	November 21, 2025	System	

PART 4 – Create Another User to See New Behavior (INTERSECTION)

1. Navigate to **Manage Users** $\rightarrow$ **Create Person**.

2. Create user **Ima Join** (Preferred User ID: ijoin).

3. Assign the Organizational Role **JKE System Admin** and set the Title to **Manager**.

4. Submit the user.

5. On the Linux terminal, check the groups assigned to ijoin.

   - **Expected Output (INTERSECTION):** Only the group common to the Mandatory lists of *both* policies: printadmin.

PART 5 – Revert Join Behavior Back to UNION

1. Navigate to **Configure System** $\rightarrow$ **Configure Policy Join Behaviors**.

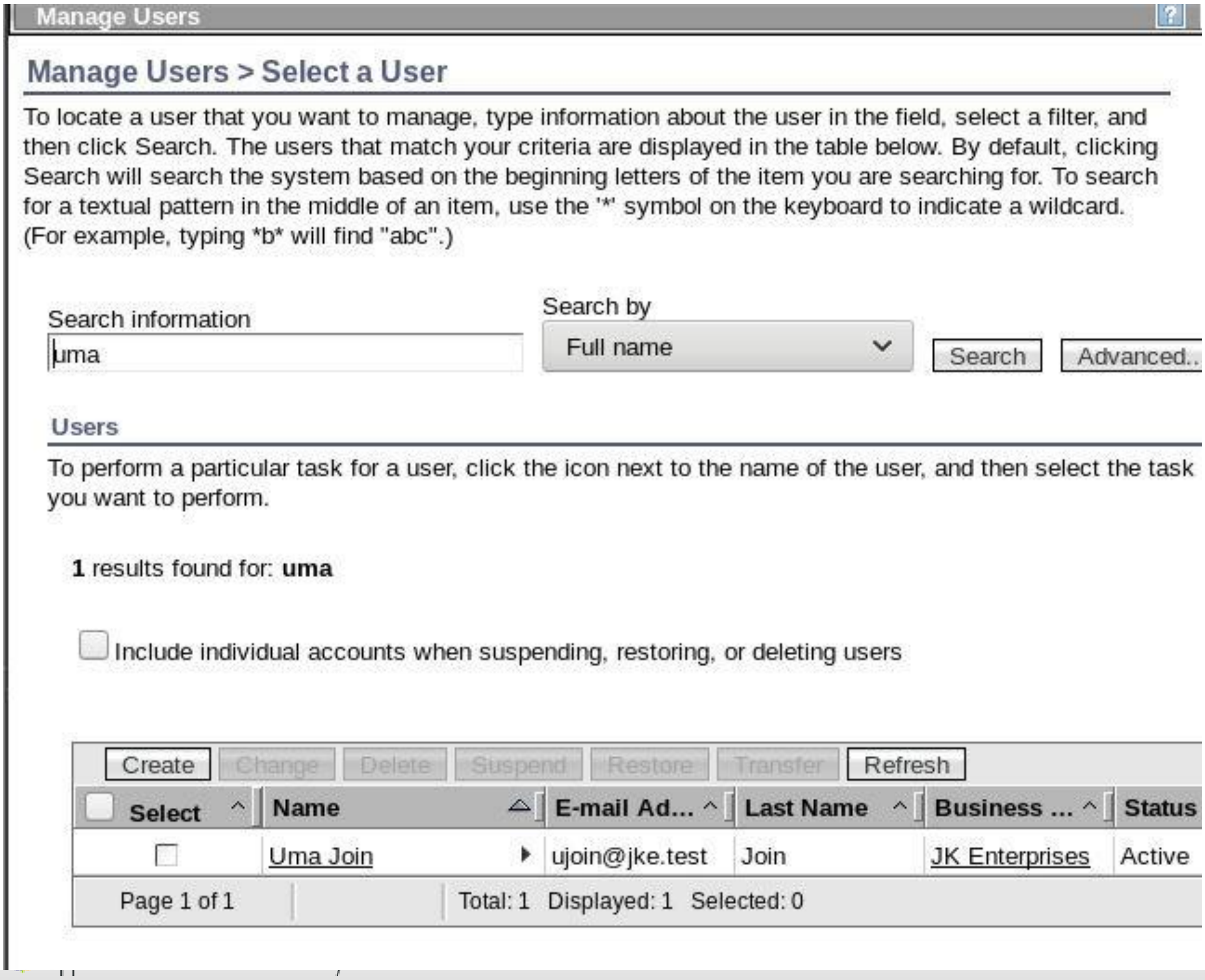
2. Open the configuration via Java Webstart.

3. Select **Service Type**: **PosixLinuxProfile**.

4. Select attribute: erposixsecondgroup.

5. Change **Join Type** back to **Union**.

6. Click **Save** and close the window.
7. **Restart ISIM Server** again.



Manage Users

Manage Users > Select a User

To locate a user that you want to manage, type information about the user in the field, select a filter, and then click Search. The users that match your criteria are displayed in the table below. By default, clicking Search will search the system based on the beginning letters of the item you are searching for. To search for a textual pattern in the middle of an item, use the '*' symbol on the keyboard to indicate a wildcard. (For example, typing *b* will find "abc".)

Search information: uma

Search by: Full name

Users

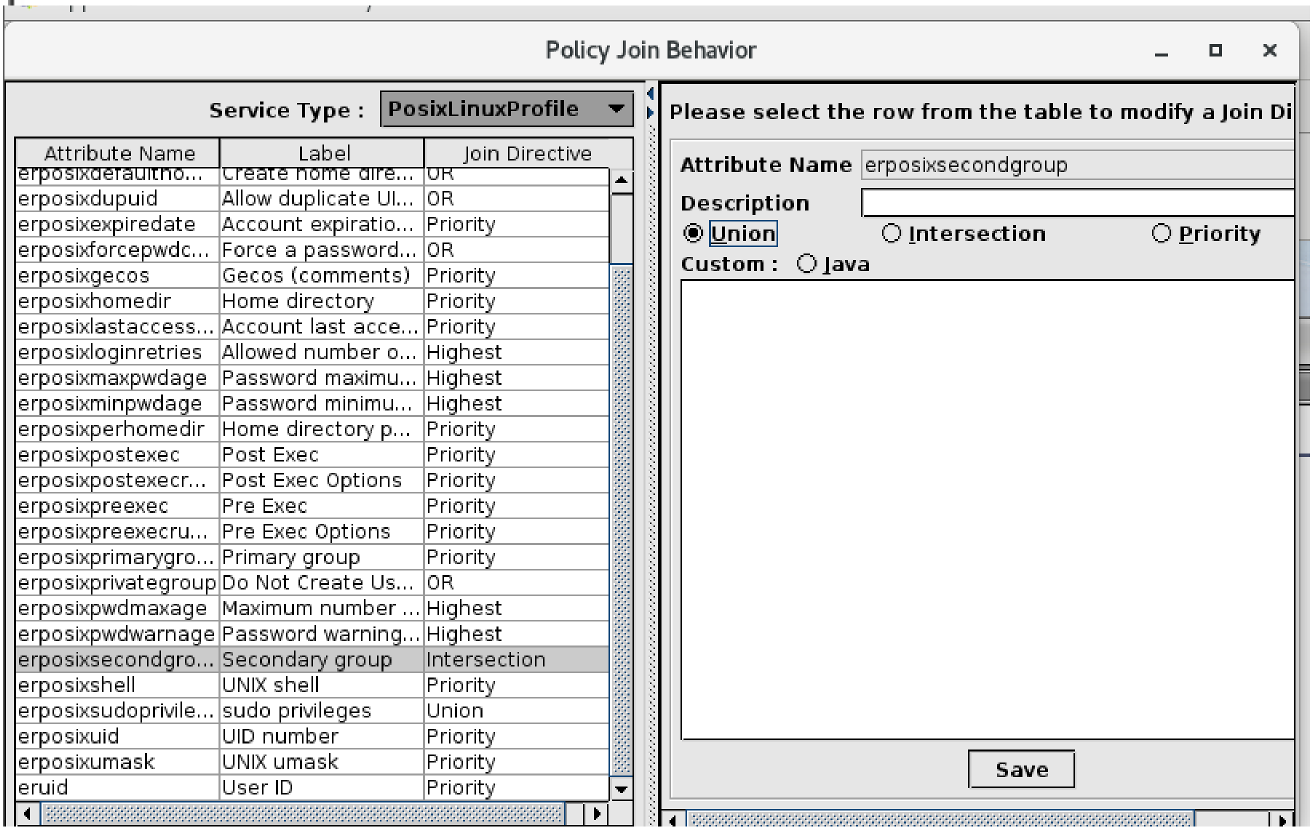
To perform a particular task for a user, click the icon next to the name of the user, and then select the task you want to perform.

1 results found for: **uma**

□ Include individual accounts when suspending, restoring, or deleting users

Select	Name	E-mail Ad...	Last Name	Business ...	Status
□	Uma Join	ujoin@jke.test	Join	JK Enterprises	Active

Page 1 of 1 Total: 1 Displayed: 1 Selected: 0



Policy Join Behavior

Service Type : PosixLinuxProfile

Attribute Name	Label	Join Directive
erposixdefaultho...	Create home dire...	OR
erposixdupuid	Allow duplicate UI...	OR
erposixexpiredate	Account expiratio...	Priority
erposixforcepwdc...	Force a password...	OR
erposixgecos	Gecos (comments)	Priority
erposixhomedir	Home directory	Priority
erposixlastaccess...	Account last acce...	Priority
erposixloginretries	Allowed number o...	Highest
erposixmaxpwdage	Password maximu...	Highest
erposixminpwdage	Password minimu...	Highest
erposixperhomedir	Home directory p...	Priority
erposixpostexec	Post Exec	Priority
erposixpostexecr...	Post Exec Options	Priority
erposixpreexec	Pre Exec	Priority
erposixpreexecru...	Pre Exec Options	Priority
erposixprimarygro...	Primary group	Priority
erposixprivategroup	Do Not Create Us...	OR
erposixpwdmaxage	Maximum number ...	Highest
erposixpwdwarnage	Password warning...	Highest
erposixsecondgro...	Secondary group	Intersection
erposixshell	UNIX shell	Priority
erposixsudoprivile...	sudo privileges	Union
erposixuid	UID number	Priority
erposixumask	UNIX umask	Priority
eruid	User ID	Priority

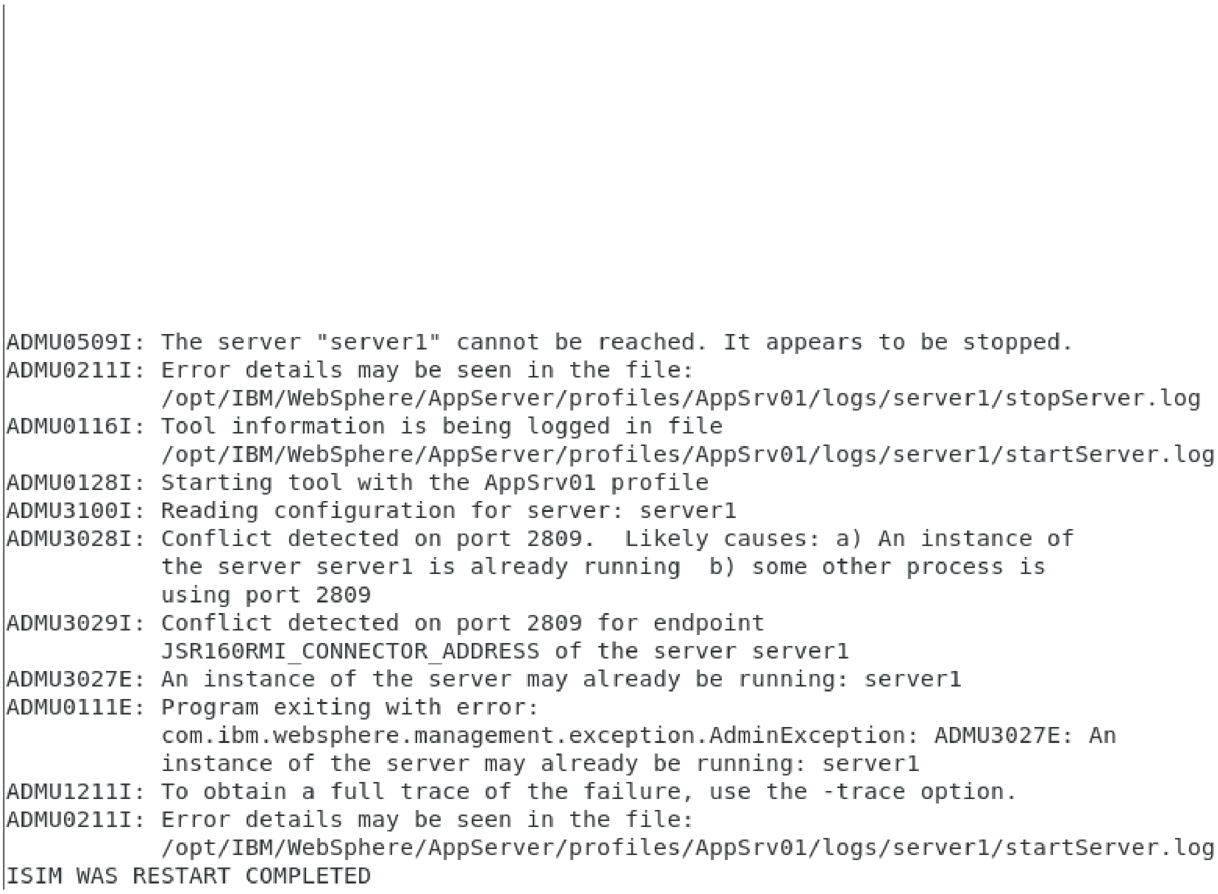
Please select the row from the table to modify a Join Di

Attribute Name: erposixsecondgroup

Description:

● Union ○ Intersection ○ Priority

Custom : ○ Java



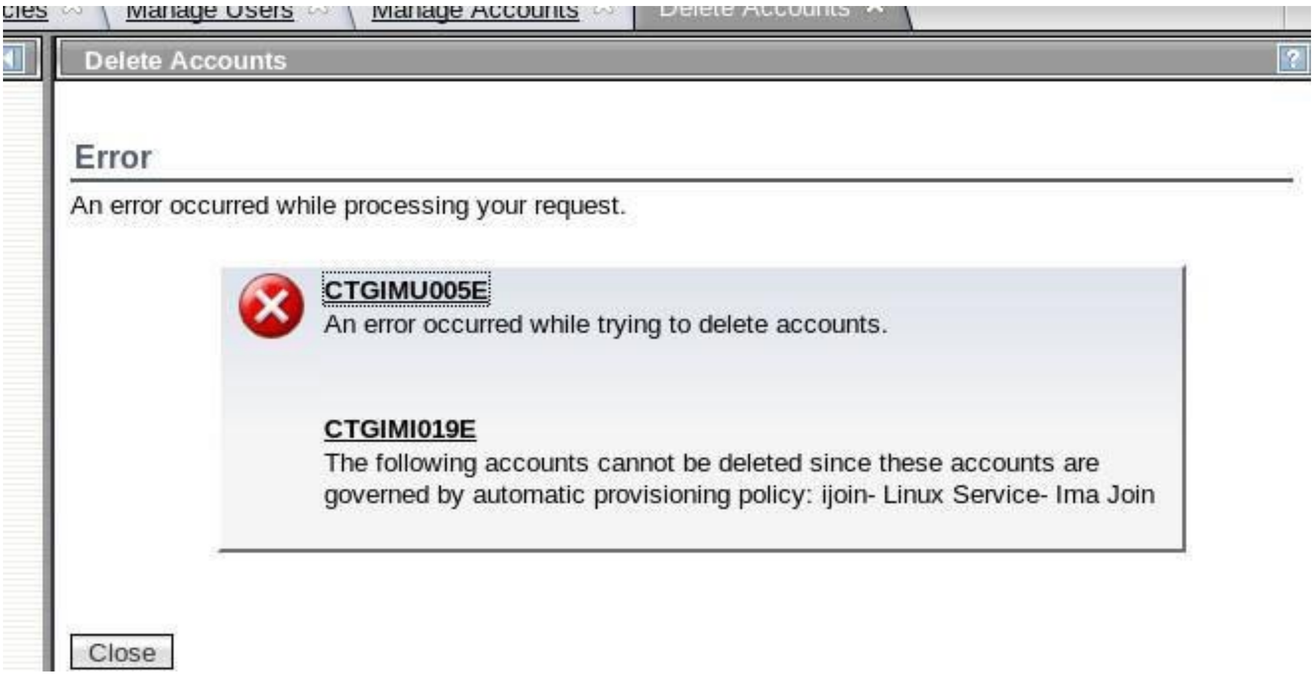
```
ADMU0509I: The server "server1" cannot be reached. It appears to be stopped.
ADMU0211I: Error details may be seen in the file:
           /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/stopServer.log
ADMU0116I: Tool information is being logged in file
           /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/startServer.log
ADMU0128I: Starting tool with the AppSrv01 profile
ADMU3100I: Reading configuration for server: server1
ADMU3028I: Conflict detected on port 2809.  Likely causes: a) An instance of
           the server server1 is already running  b) some other process is
           using port 2809
ADMU3029I: Conflict detected on port 2809 for endpoint
           JSR160RMI_CONNECTOR_ADDRESS of the server server1
ADMU3027E: An instance of the server may already be running: server1
ADMU0111E: Program exiting with error:
           com.ibm.websphere.management.exception.AdminException: ADMU3027E: An
           instance of the server may already be running: server1
ADMU1211I: To obtain a full trace of the failure, use the -trace option.
ADMU0211I: Error details may be seen in the file:
           /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/startServer.log
ISIM WAS RESTART COMPLETED
```

Exercise 7.9 – De-provisioning an Account

Objective: Delete Ima Join's Linux

account.

1. Navigate to **Manage Users** $\rightarrow$ **Ima Join** $\rightarrow$ **Accounts** tab.
2. Select the Linux account and choose the **Delete** action.
3. Observe the outcome, which depends on the provisioning policy's allowance settings (if deletion is prohibited, allowed, or requires a workflow).



Error

An error occurred while processing your request.

CTGIMU005E

An error occurred while trying to delete accounts.

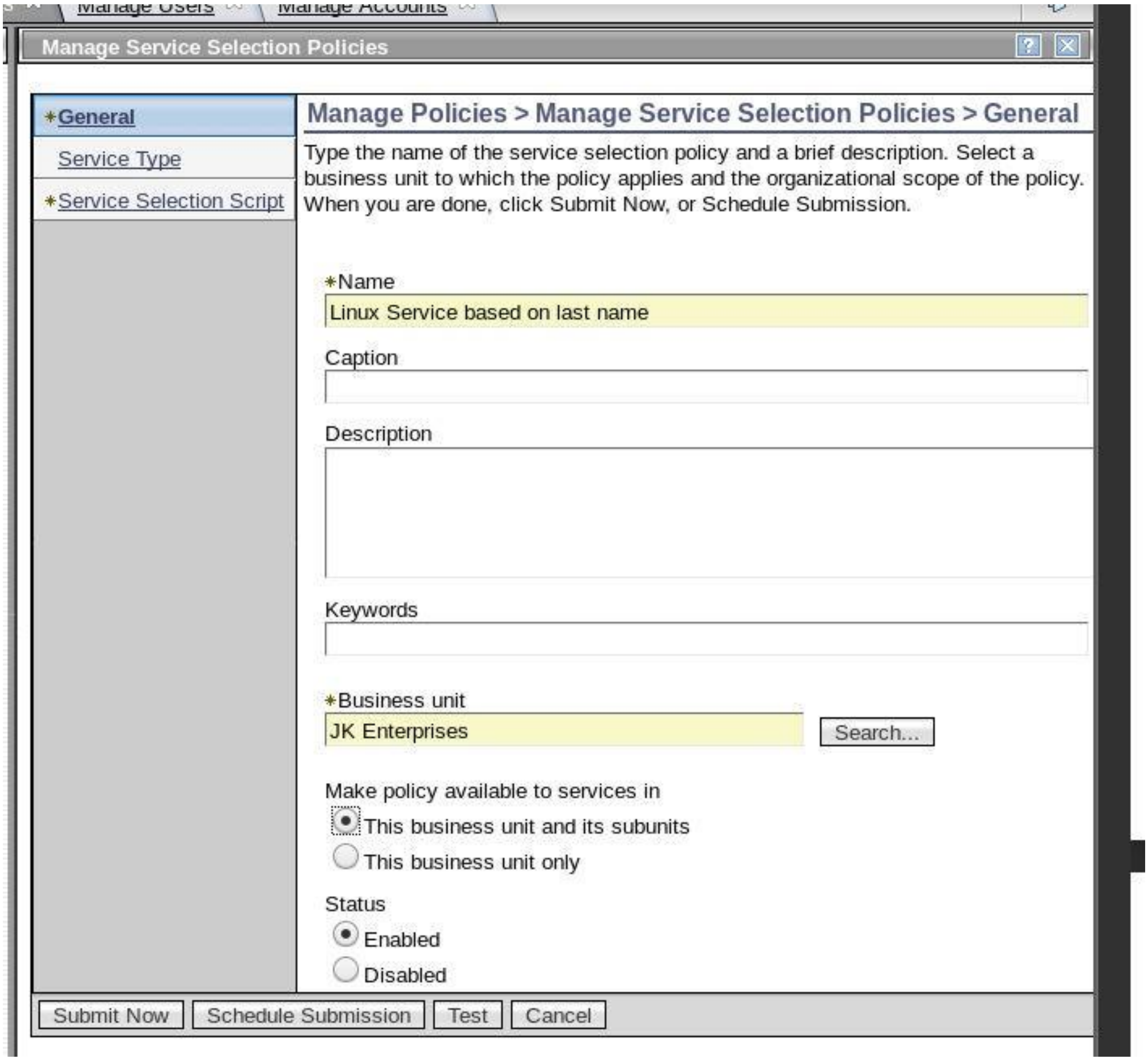
CTGIMI019E

The following accounts cannot be deleted since these accounts are governed by automatic provisioning policy: ijoin- Linux Service- Ima Join

Exercise 7.10 – Creating a Service Selection Policy

Objective: Select the Linux Service automatically based on the last name (M–Z).

1. Navigate to the service selection policy configuration area (location may vary depending on ISIM version).
2. Create a new Service Selection Policy.
3. Define a script or rule that evaluates the user's last name. The script should return the **Linux Service** object for users whose last name begins with a letter from M through Z, and return nothing for A through L.



Manage Policies > Manage Service Selection Policies > General

Type the name of the service selection policy and a brief description. Select a business unit to which the policy applies and the organizational scope of the policy. When you are done, click Submit Now, or Schedule Submission.

*Name: Linux Service based on last name

Caption:

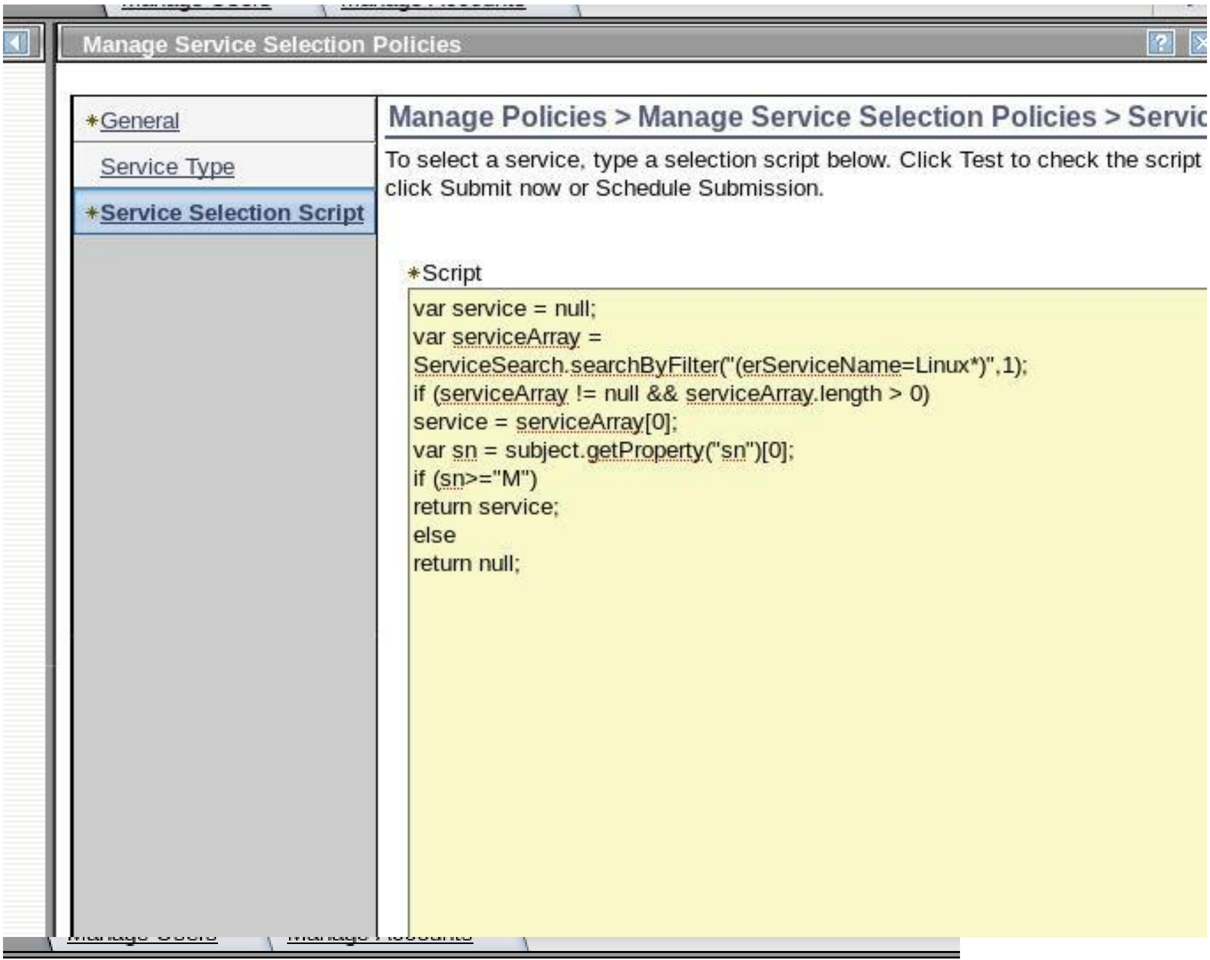
Description:

Keywords:

*Business unit: JK Enterprises

Make policy available to services in
● This business unit and its subunits
○ This business unit only

Status
● Enabled
○ Disabled

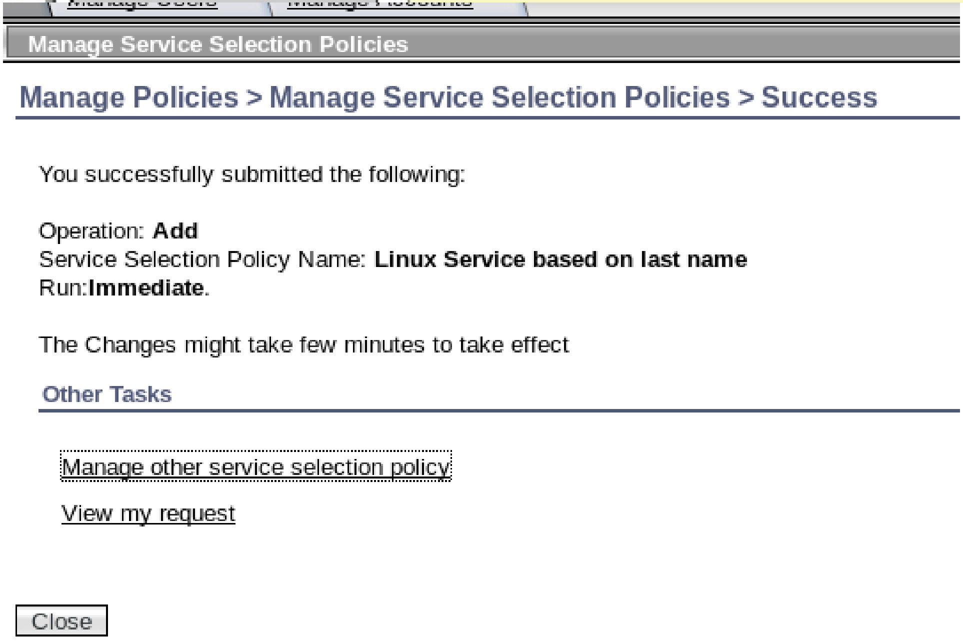


Manage Policies > Manage Service Selection Policies > Servic

To select a service, type a selection script below. Click Test to check the script click Submit now or Schedule Submission.

*Script

```
var service = null;
var serviceArray =
ServiceSearch.searchByFilter("(erServiceName=Linux*)",1);
if (serviceArray != null && serviceArray.length > 0)
service = serviceArray[0];
var sn = subject.getProperty("sn")[0];
if (sn>="M")
return service;
else
return null;
```


Manage Service Selection Policies

Manage Policies > Manage Service Selection Policies > Success

You successfully submitted the following:

Operation: **Add**
Service Selection Policy Name: **Linux Service based on last name**
Run:**Immediate**.

The Changes might take few minutes to take effect

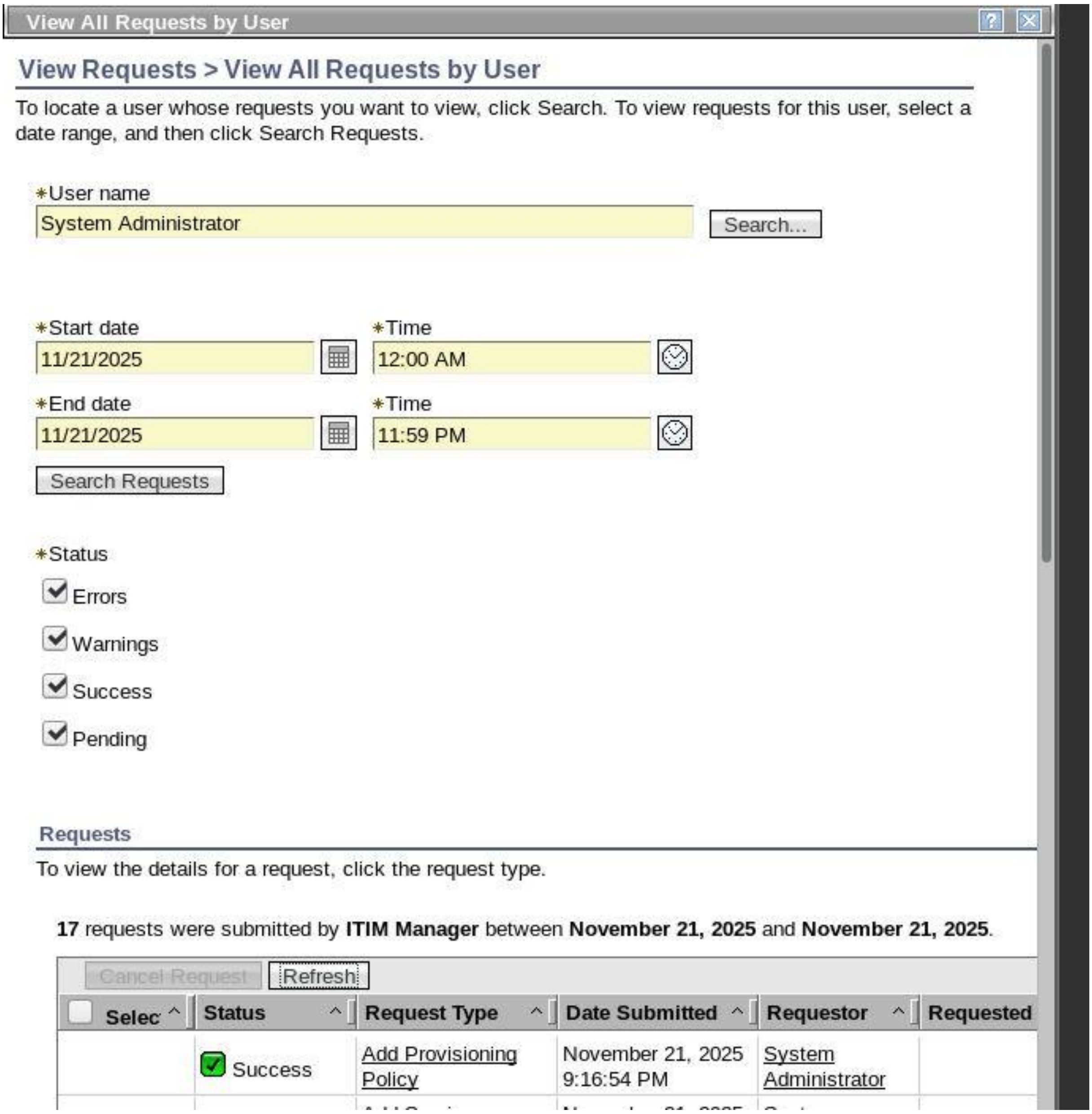
Other Tasks
Manage other service selection policy
View my request
Close

Exercise 7.11 – Provisioning Policy Using Service Selection Policy

Objective: Provision Linux accounts for users whose last name begins with M–Z.

1. Create a new provisioning policy.

2. Set the policy details as follows:
   - Set **Policy Name** to **M–Z Linux Accounts**.
   - Set **Priority** to **1000**.
   - Set **Members** to **All users**.
3. In **Entitlements Configuration**, set the **Target** to the **Service Selection Policy** created in Exercise 7.10.
4. Submit and enforce the policy.
5. **Result:** Only users with a last name starting M–Z receive Linux accounts.



View Requests > View All Requests by User

To locate a user whose requests you want to view, click Search. To view requests for this user, select a date range, and then click Search Requests.

*User name: System Administrator

*Start date: 11/21/2025 *Time: 12:00 AM

*End date: 11/21/2025 *Time: 11:59 PM

*Status

☑ Errors

☑ Warnings

☑ Success

☑ Pending

Requests

To view the details for a request, click the request type.

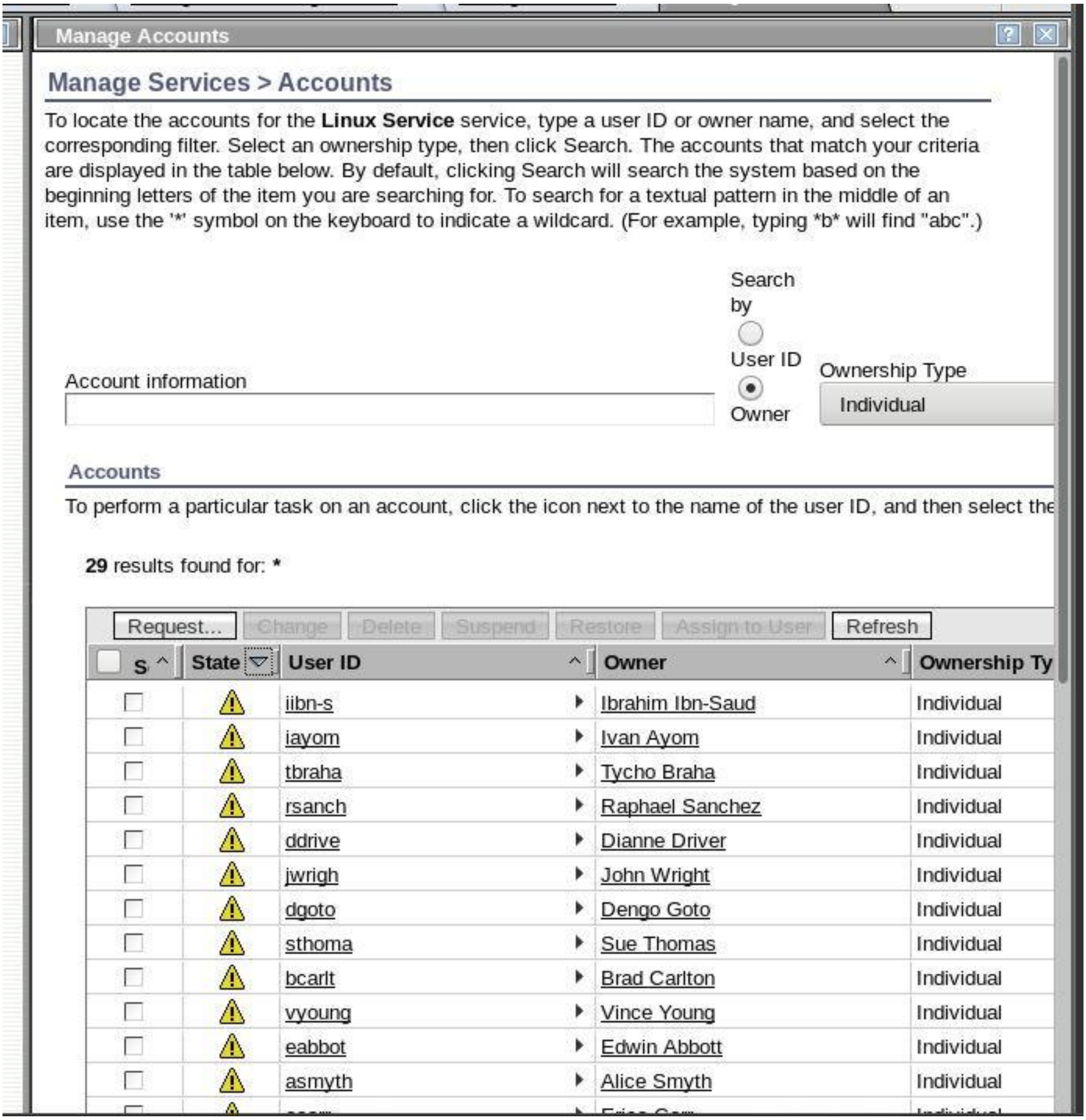
17 requests were submitted by **ITIM Manager** between **November 21, 2025** and **November 21, 2025**.

□ Selec	Status	Request Type	Date Submitted	Requestor	Requested
	✓ Success	Add Provisioning Policy	November 21, 2025 9:16:54 PM	System Administrator	

Objective: Automatically correct non-compliant accounts.

1. Navigate to the provisioning policy (e.g., *Manager Linux Accounts*) and view the non- compliant accounts (State column).

2. Change the policy's **Enforcement** mode from **Mark** to **Correct**.



Manage Services > Accounts

To locate the accounts for the **Linux Service** service, type a user ID or owner name, and select the corresponding filter. Select an ownership type, then click Search. The accounts that match your criteria are displayed in the table below. By default, clicking Search will search the system based on the beginning letters of the item you are searching for. To search for a textual pattern in the middle of an item, use the '*' symbol on the keyboard to indicate a wildcard. (For example, typing *b* will find "abc".)

Account information

Search by ○ User ID ● Owner

Ownership Type: Individual

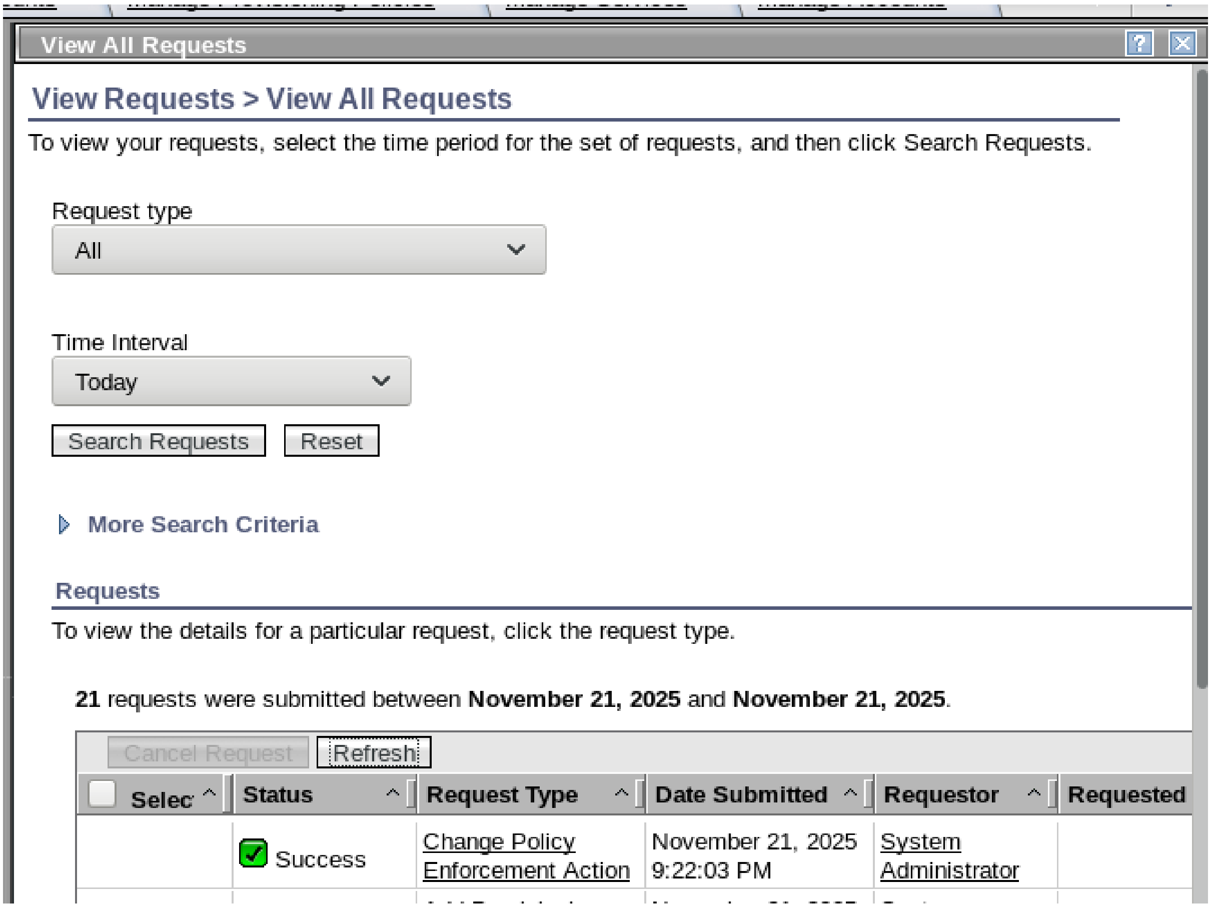
Accounts

To perform a particular task on an account, click the icon next to the name of the user ID, and then select the

29 results found for: *

S	State	User ID	Owner	Ownership Ty
□	⚠	iibn-s	Ibrahim Ibn-Saud	Individual
□	⚠	iayom	Ivan Ayom	Individual
□	⚠	tbraha	Tycho Braha	Individual
□	⚠	rsanch	Raphael Sanchez	Individual
□	⚠	ddrive	Dianne Driver	Individual
□	⚠	jwrigh	John Wright	Individual
□	⚠	dgoto	Dengo Goto	Individual
□	⚠	sthoma	Sue Thomas	Individual
□	⚠	bcarlt	Brad Carlton	Individual
□	⚠	vyoung	Vince Young	Individual
□	⚠	eabbot	Edwin Abbott	Individual
□	⚠	asmyth	Alice Smyth	Individual

3. Submit and enforce the policy.



View All Requests

View Requests > View All Requests

To view your requests, select the time period for the set of requests, and then click Search Requests.

Request type: All

Time Interval: Today

Requests

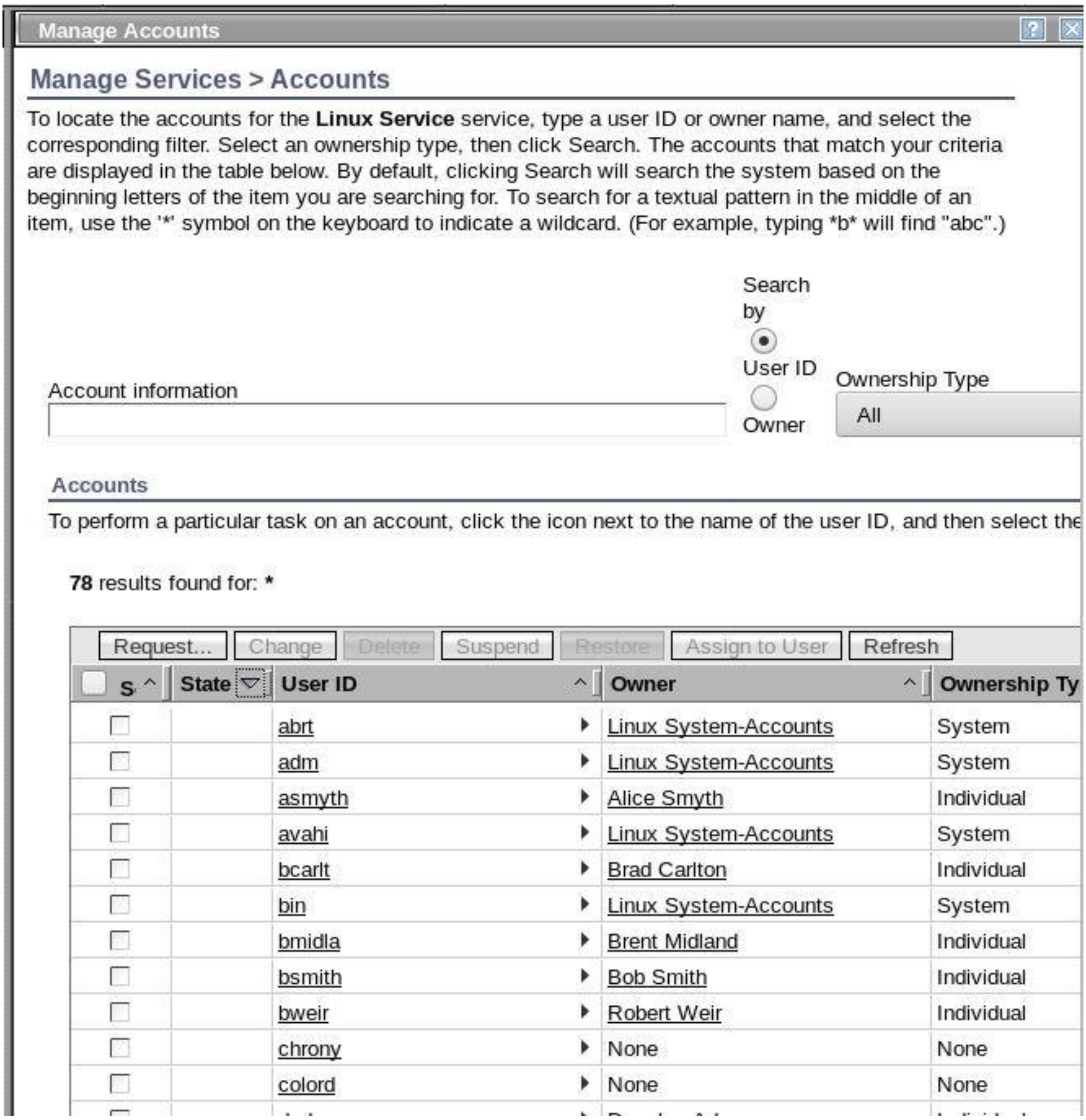
To view the details for a particular request, click the request type.

21 requests were submitted between **November 21, 2025** and **November 21, 2025**.

□ Select	Status	Request Type	Date Submitted	Requestor	Requested
	✓ Success	Change Policy Enforcement Action	November 21, 2025 9:22:03 PM	System Administrator	

4. The system will now automatically submit requests to fix all violations (e.g., change the Shell for Douglas Adams to /bin/ksh).

5. Verify that the accounts are now compliant.



Manage Services > Accounts

To locate the accounts for the **Linux Service** service, type a user ID or owner name, and select the corresponding filter. Select an ownership type, then click Search. The accounts that match your criteria are displayed in the table below. By default, clicking Search will search the system based on the beginning letters of the item you are searching for. To search for a textual pattern in the middle of an item, use the '*' symbol on the keyboard to indicate a wildcard. (For example, typing *b* will find "abc".)

Account information

Search by ● User ID ○ Owner

Ownership Type: All

Accounts

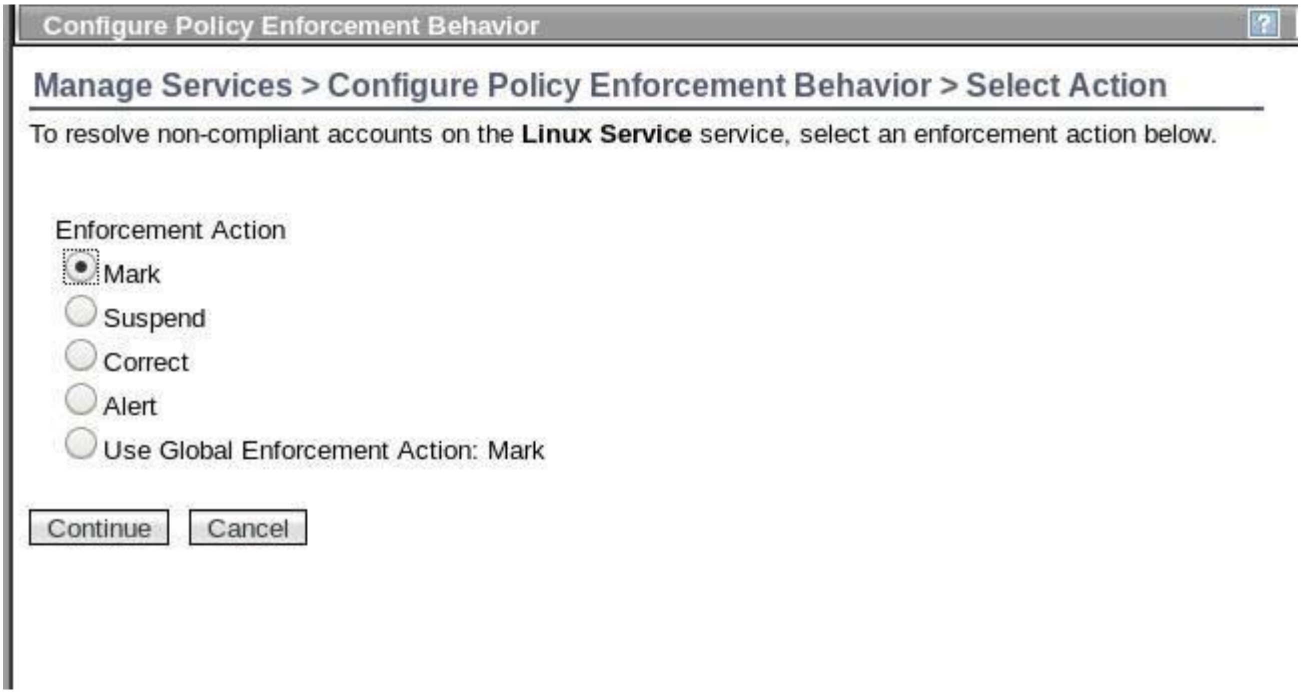
To perform a particular task on an account, click the icon next to the name of the user ID, and then select the

78 results found for: *

Request... Change Delete Suspend Restore Assign to User Refresh

□ S	State	User ID	Owner	Ownership Ty
□		abrt	Linux System-Accounts	System
□		adm	Linux System-Accounts	System
□		asmyth	Alice Smyth	Individual
□		avahi	Linux System-Accounts	System
□		bcarlt	Brad Carlton	Individual
□		bin	Linux System-Accounts	System
□		bmidla	Brent Midland	Individual
□		bsmith	Bob Smith	Individual
□		bweir	Robert Weir	Individual
□		chrony	None	None
□		colord	None	None

6. Revert the **Enforcement** mode back to **Mark**.



Configure Policy Enforcement Behavior

Manage Services > Configure Policy Enforcement Behavior > Select Action

To resolve non-compliant accounts on the **Linux Service** service, select an enforcement action below.

Enforcement Action

● Mark

○ Suspend

○ Correct

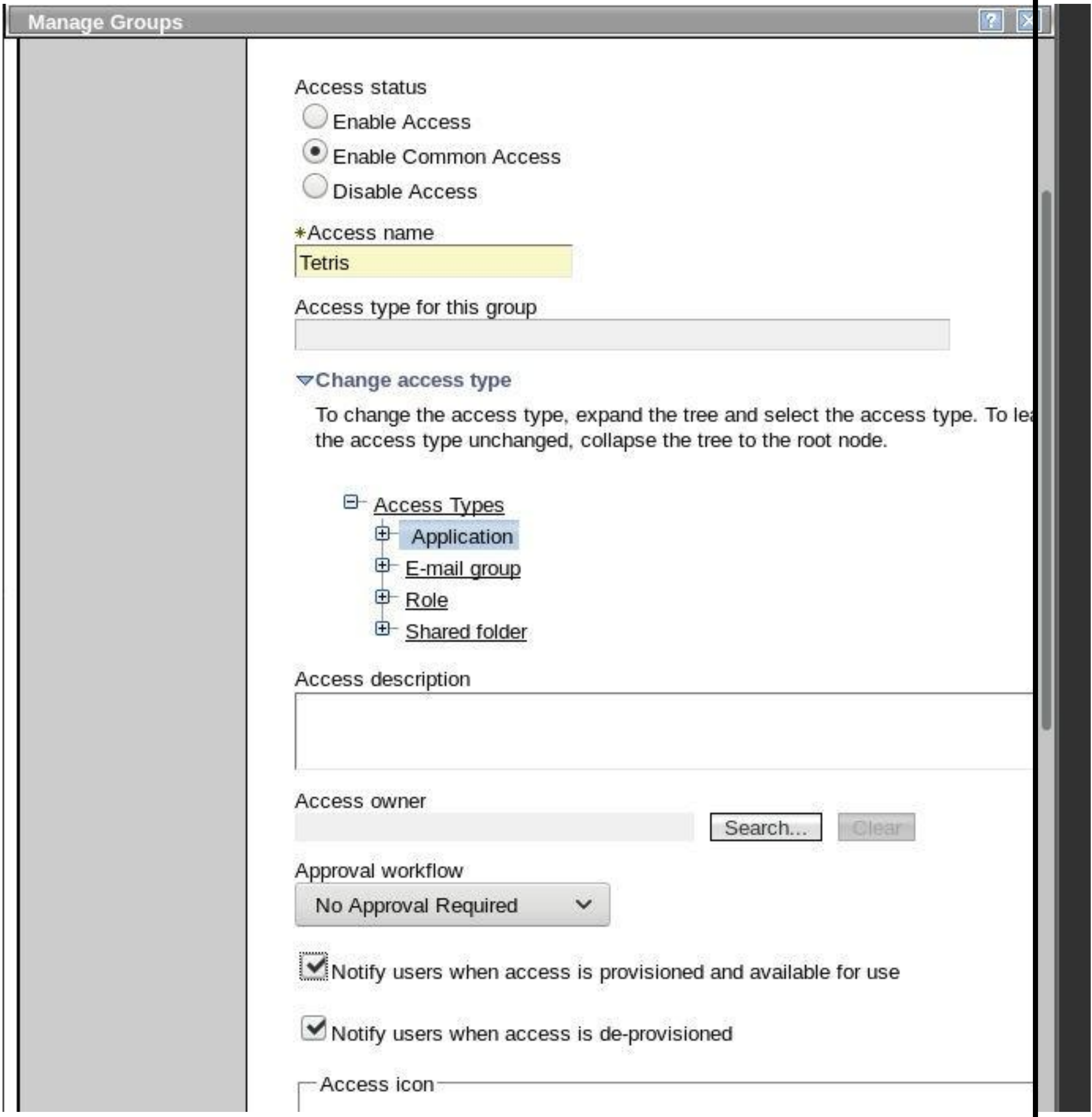
○ Alert

○ Use Global Enforcement Action: Mark

Exercise 7.13 – Provisioning Access on Linux

Objective: Create and request an application access (Tetris) based on a Linux group.

1. Navigate to the Linux Service $\rightarrow$ **Manage Groups**.
2. Select the games group $\rightarrow$ **Define Access**.
3. Enable **Common Access** and set the **Name** to **Tetris**.
4. Login as the user asmith (Alice Smyth).
5. Navigate to the **Request Access** screen.



Access status

○ Enable Access

● Enable Common Access

○ Disable Access

*Access name

Tetris

Access type for this group

To change the access type, expand the tree and select the access type. To lea the access type unchanged, collapse the tree to the root node.

Access description

Access owner

Approval workflow

No Approval Required

☑ Notify users when access is provisioned and available for use

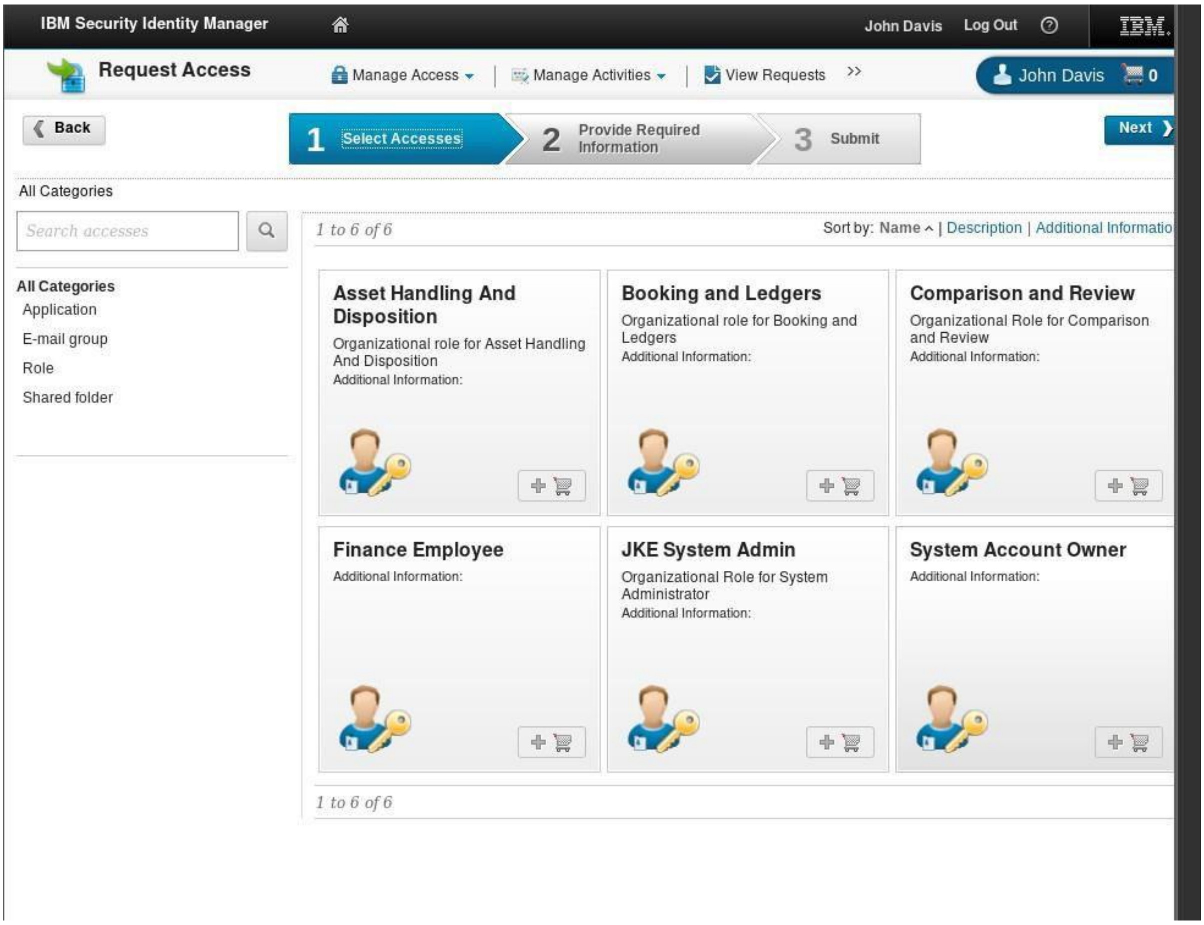
☑ Notify users when access is de-provisioned

6. Request the **Tetris** access and **Submit**.

7. *Verification:* Confirm asmith is added to the games group on Linux.

8. Login as user jdavis.

9. Navigate to **Request Access** and confirm that the **Tetris** access is **not visible** (as jdavis is not entitled by policy).



Asset Handling And Disposition
Organizational role for Asset Handling And Disposition
Additional Information:

Booking and Ledgers
Organizational role for Booking and Ledgers
Additional Information:

Comparison and Review
Organizational Role for Comparison and Review
Additional Information:

Finance Employee
Additional Information:

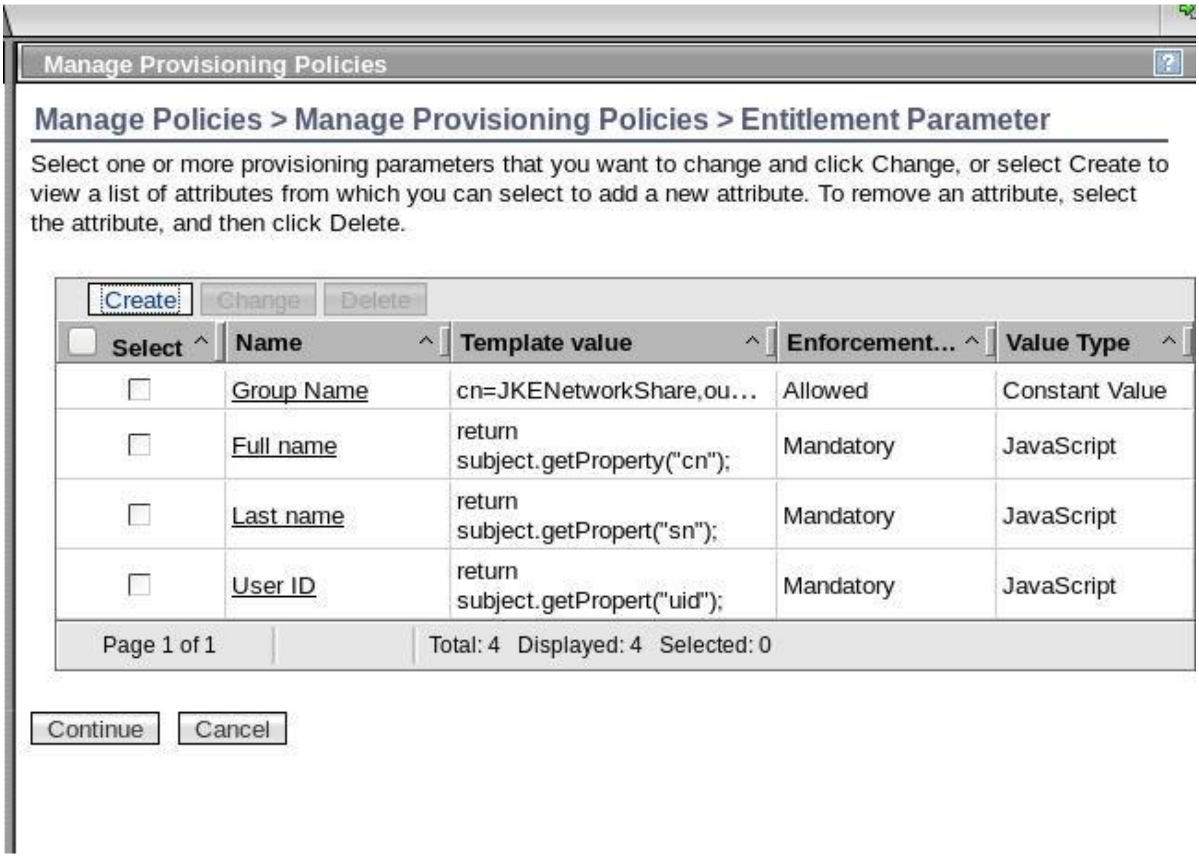
JKE System Admin
Organizational Role for System Administrator
Additional Information:

System Account Owner
Additional Information:

1 to 6 of 6

Exercise 7.14 – Provisioning Shared Folder Access on LDAP Objective: Provide LDAP-based shared directory access.

1. Modify the provisioning policy for the **TechSupport LDAP** service.
2. Set entitlement parameters for the LDAP service:
   - Set **Group Name** to **JKENetworkShare**.
   - Use JavaScript for mapping attributes like Full Name, Last Name, and User ID.
3. Define Access for the JKENetworkShare group: **TechSupport Shared Directory**.

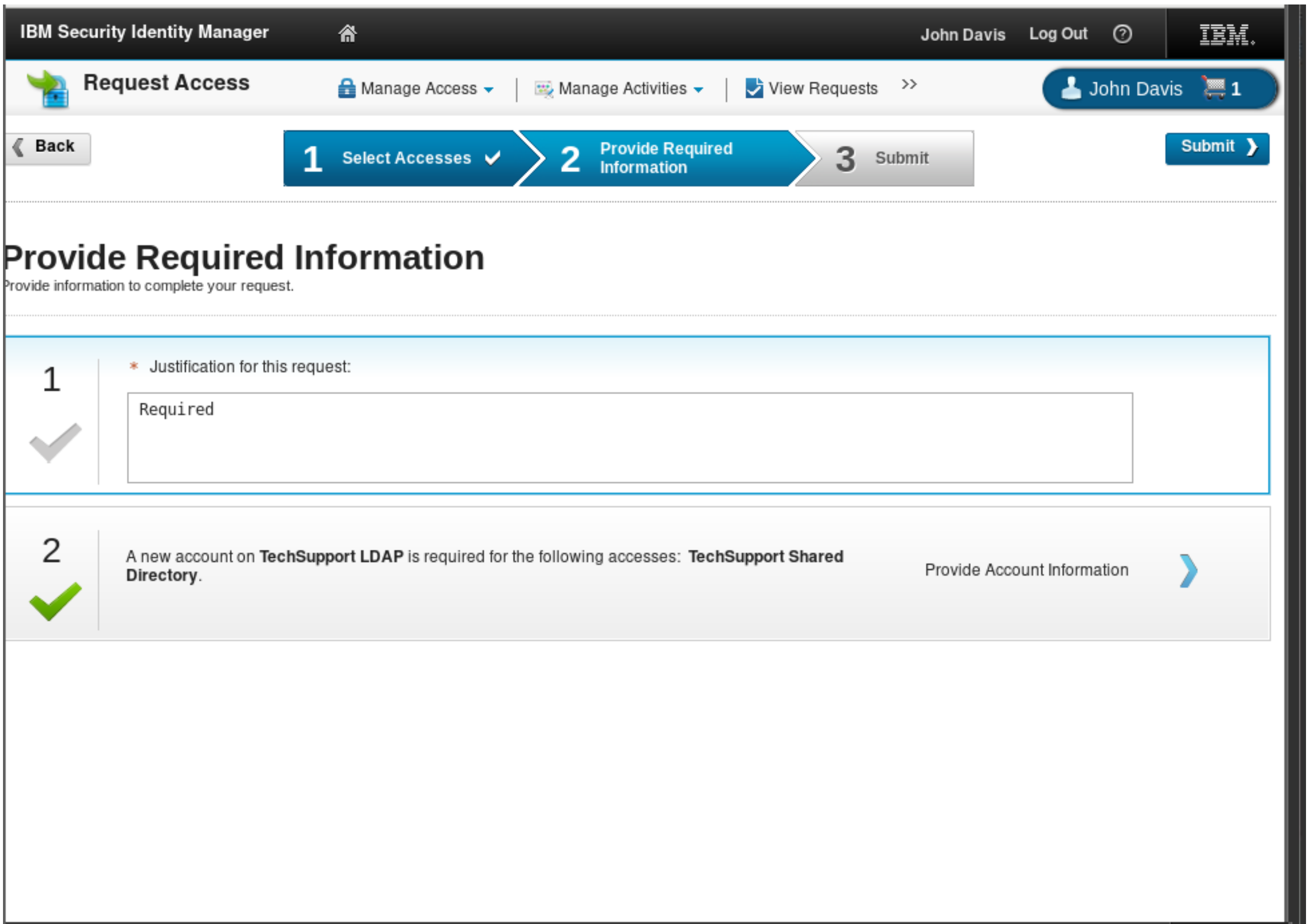


Manage Policies > Manage Provisioning Policies > Entitlement Parameter

Select one or more provisioning parameters that you want to change and click Change, or select Create to view a list of attributes from which you can select to add a new attribute. To remove an attribute, select the attribute, and then click Delete.

Select	Name	Template value	Enforcement...	Value Type
□	Group Name	cn=JKENetworkShare,ou...	Allowed	Constant Value
□	Full name	return subject.getProperty("cn");	Mandatory	JavaScript
□	Last name	return subject.getPropert("sn");	Mandatory	JavaScript
□	User ID	return subject.getPropert("uid");	Mandatory	JavaScript

Page 1 of 1 Total: 4 Displayed: 4 Selected: 0



Provide Required Information

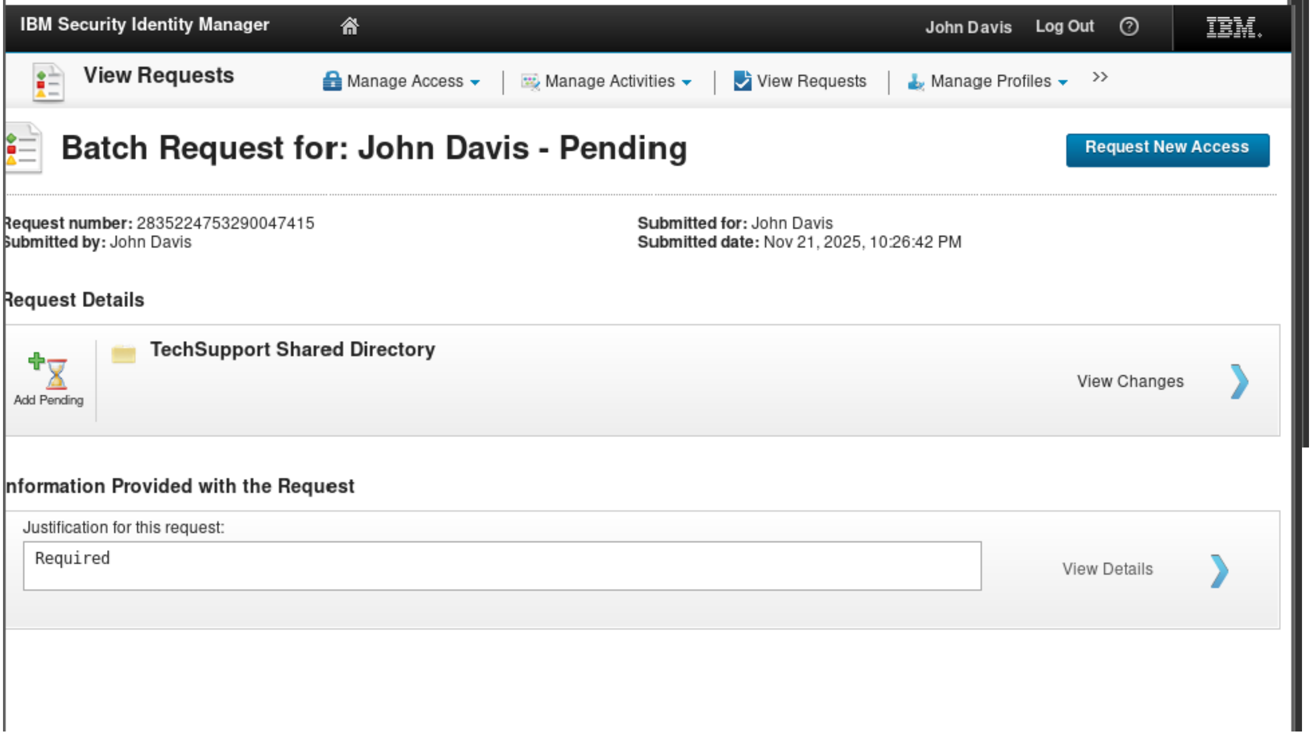
Provide information to complete your request.

1 * Justification for this request:

```
Required
```

2 A new account on **TechSupport LDAP** is required for the following accesses: **TechSupport Shared Directory**.

Provide Account Information



Batch Request for: John Davis - Pending

Request number: 2835224753290047415
Submitted by: John Davis
Submitted for: John Davis
Submitted date: Nov 21, 2025, 10:26:42 PM

Request Details

Add Pending — **TechSupport Shared Directory** — View Changes

Information Provided with the Request

Justification for this request:

```
Required
```

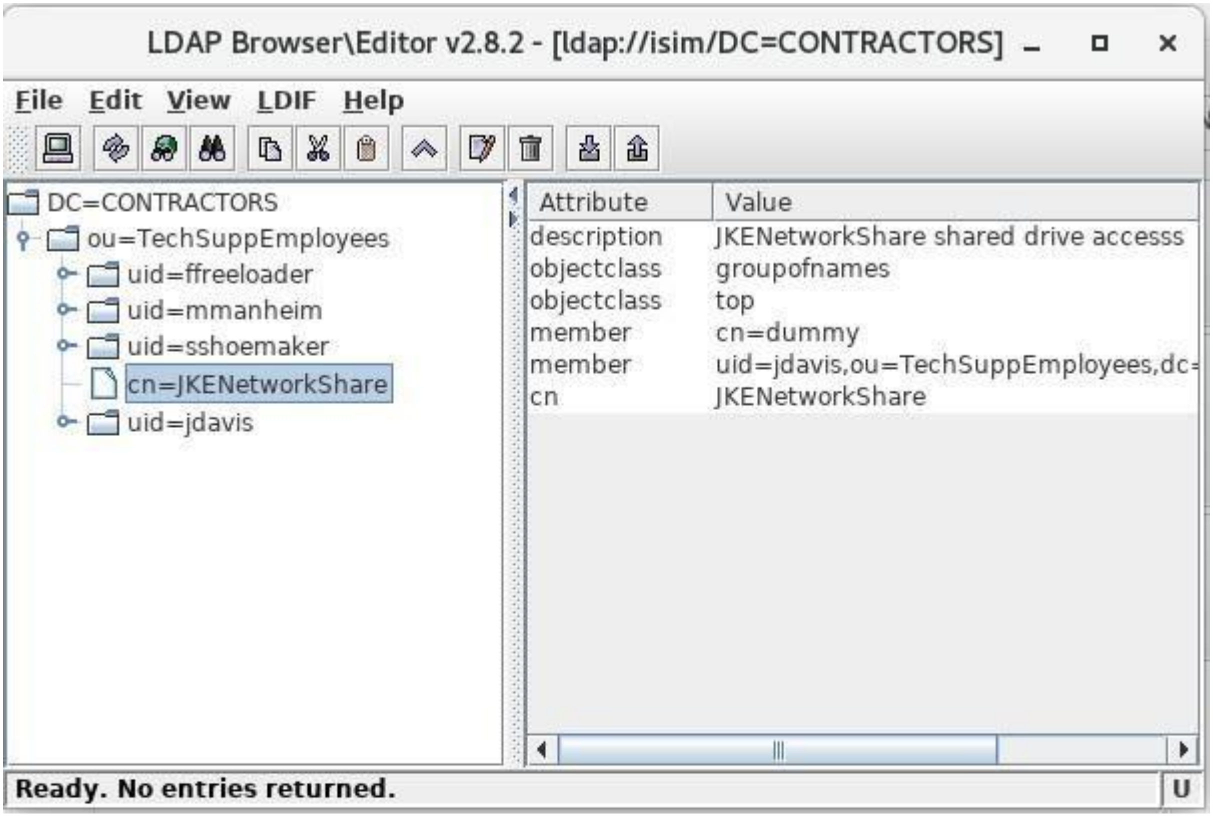
View Details

4. Login as user jdavis.

5. Navigate to **Request Access** and request the **TechSupport Shared Directory** access.

6. ISIM will automatically provision an LDAP account (if necessary) and grant access by adding jdavis to the JKENetworkShare group.

7. Confirm the user and group membership in an **LDAP Browser**.



```
DC=CONTRACTORS
  ou=TechSuppEmployees
    uid=ffreeloader
    uid=mmanheim
    uid=sshoemaker
    cn=JKENetworkShare
    uid=jdavis
```

Attribute	Value
description	JKENetworkShare shared drive accesss
objectclass	groupofnames
objectclass	top
member	cn=dummy
member	uid=jdavis,ou=TechSuppEmployees,dc=
cn	JKENetworkShare

Ready. No entries returned.

Conclusion

The exercises successfully demonstrated the configuration and verification of provisioning policies for Linux and LDAP services, implementation of identity, password, adoption, and service selection policies, and verification of provisioning, compliance, and access request workflows to achieve full lifecycle governance in ISIM.