Using the Core Access Assurance Suite™ Sample Workflows

Core Access Assurance Suite 9.1

Core Security

1000 Holcomb Woods Parkway Suite 401
Roswell, GA 30076
Domestic: (678) 304-4500
Fax: (770) 573-3743

Trademarks

Table of Contents

List of Figures

Chapter 1: Introduction

The Core Access Assurance Suite solution includes sample workflows designed to demonstrate the functionality of the different products in the suite. You can choose one or more of the sample workflows to install during the Express Configuration process. By default, all sample workflows are installed. Once installed, the sample workflows are fully functional with the targets already configured. For details on the installation process, see the manual *Installing the Access Assurance Suite*.

You can use the sample workflows as templates that you can easily customize for your specific requirements. This manual demonstrates the functionality of these workflows by walking you step by step through the various forms that are configured in the individual workflows.

Functionality of the Sample Workflows

Each sample workflow offers different functionality. With the exception of the CourionSelfService Password Reset workflow, each of the workflows presents two or more possible provisioning actions that can be selected by the end user/provisioner.

In addition to the sample workflows listed in Table 1, the Access Assurance Suite also includes a workflow template that you can customize to implement Transparent Synchronization at your site (CourionTransparentSync Reset). See the *Access Assurance Suite Implementation Guide* for information about how to configure the Transparent Synchronization feature and customize this workflow template.

Table 1: Courion Sample Workflows

Workflow	Description	Available Actions
CourionSelfService	Enables end users to claim their accounts on various systems. Users must claim accounts to populate the IdentityMap, which is used by the other workflows.	Change View
CourionSelfService Profile Management	Enables end users to create a profile for themselves. The profile includes information that AccountCourier uses when it creates an account. The profile also includes secret challenge/ response questions and answers used for resetting a password when running the CourionSelfService Password reset workflow.	Add Change
CourionSelfService Password Reset	Enables end users to reset their password even if they have forgotten their current password.	Password Reset
Courion Compliance	Enables a provisioner[1] to view details of user accounts, grouped according to compliance status, and then accept or reject that status.	Verify

Table 1: Courion Sample Workflows

Workflow	Description	Available Actions
CourionSuper-User	Enables a provisioner to create accounts for a new employee, or perform a variety of actions on existing accounts.	Create Add Change Delete Disable Enable View
Core Role Creation	Enables a provisioner to create a new role and associated template accounts by mining existing user's accounts, and to add additional template accounts to an existing role definition.	Create Add
Core Role Management	Enables a provisioner to create a new role based on an existing role Additionally, a provisioner can perform a variety of actions on an existing role.	Create Change Delete Disable Enable

1. A provisioner can provision accounts or resources (create, add, change, enable, disable, and delete), either with or without an approval, depending on the design of the workflow

Workflow Dependencies

Some sample workflows require that you run other sample workflows first for them to execute properly.

CourionSelf-Service, CourionCompliance, CourionSuper-User, and Role Management

You need to run the Courion Self-Service Claim Accounts workflow to claim resources and populate the IdentityMap before you run the Compliance Review and Role Management workflows and before you use the Super User Change Accounts workflow. You can use other Super User workflows without first running Self-Service Claim Accounts.

CourionSelf-Service Profile Management and CourionSelf-Service Password Reset

You need to run the Self-Service Profile Management workflow to build a profile before you run the Self-Service Password Reset workflow.

Access Key Requirements for the Sample Workflows

The sample workflows require certain access keys as well as access keys for the following connectors:

- Microsoft Windows® Active Directory
- Microsoft Exchange®

- Netscape® SMTP

The sample workflows and the access keys they require are:

- **CourionSelfService** — AccountCourier®
- **CourionSelfService Profile Management** — ProfileCourier®
- **CourionSelfService Password Reset** — PasswordCourier®
- **Courion Compliance** — ComplianceCourier™
- **CourionSuper-User** — AccountCourier
- **Courion Role Creation** — RoleCourier®
- **Courion Role Management** — RoleCourier
- **CourionTransparentSync Reset** workflow template — PasswordCourier and Transparent Synchronization.

Jump Start Workflow Options

Jump Start workflow options are pre-configured workflows designed to solve a specific business challenge. These workflows use a subset of AccountCourier and ComplianceCourier features to deliver functionality that you can use as soon as you install the Access Assurance Suite. You access Jump Start workflows from the Access Assurance Suite console page. Jump Start workflows also appear in the list of predefined sample workflows in the Administration Manager.

For more information about Jump Start Workflows, see the Jump Start workflow user guides, which you can access from the documentation roadmap. Click on **DOCUMENTATION** from the left side of the console page.

Running the Express Connector Configuration Manager

If you installed the Access Assurance Suite without running the Express Connector Configuration Manager, and you want to run it now to use the sample workflows, you can do so from the Start menu:

Start>All Programs>Core Access Assurance Suite>Express Connector Configuration Manager

Note: The Express Connector Configuration Manager is only available in a single server installation.

For information about how to enter configuration information see the manual *Installing the Access Assurance Suite.*

Copying the Sample Workflows

Core Security strongly recommends that you make a copy of an existing workflow before you edit the Administration Manager forms. You can then edit the copy and still have the original for reference. Another reason for creating a new workflow is that if you reinstall the Access Assurance Suite or upgrade to a higher version, you overwrite the preconfigured workflows, including the sample workflows. In this situation, you would lose any edits you made to the original sample workflow. For details on how to create a workflow by copying from an existing workflow, see *"Copying Sample Workflows" on page 241*.

Administration Manager Forms Not Described in this Manual

When the sample workflows are installed during Express Configuration, a number of forms are pre-configured that are not described in this manual. You can modify these forms based on your specific needs. A complete description of these forms can be found in the manual *Configuring Workflows with the Access Assurance Suite Administration Manager.* See *"References to Administration Manager Forms" on page 245* for a table which lists the sections in that manual that describe those forms.

The following sections provide information on these forms, for settings specific to the sample workflows:

- *"Authentication"*
- *"Global Settings"*
- *"Macros"*
- *"Triggers, Ticketing, and Notification"*
- *"Confirmation and Summary"*

Authentication

As configured, the sample workflows authenticate using Microsoft Active Directory authentication. If you want to use a different authentication method, you need to modify the Provisioner Community forms.

Global Settings

- **Target Configuration** — Most of the sample workflows are configured to access Active Directory logon accounts, Microsoft Exchange (for email accounts), and Microsoft ADO (for the IdentityMap). The Role Creation and Role Management workflows also access the Core Role Connector. If you need to access additional targets, they must be configured in the workflow before they can be selected by the provisioner.
- **Available Actions** — Each sample workflow has one or more actions associated with that workflow. To change the text used to describe those actions to end users, see the section on configuring Action Groups.
- **IdentityMap** — The IdentityMap keeps track of the various resources associated with each user. The IdentityMap information is stored in the UserBasedTargets table in the Transaction Repository. Retrieving information from the IdentityMap is done via the Connector for Microsoft ADO. It is unlikely you will need to change the settings for the IdentityMap.
- **Transaction Repository** — The transaction repository contains the IdentityMap information. It is also used by the Core Role Connector to store information about roles. It uses the Connector for Microsoft ADO.

Macros

The various sample workflows use custom macros to place information gathered dynamically by the Courion Server into forms and messages displayed to the end user. Information on individual macros can be found at the beginning of the chapters for the specific sample workflows.

Triggers, Ticketing, and Notification

You can associate event triggers, ticketing, and notification with a workflow.

Triggers

You can associate event triggers with the functions in a script you select during the Connector for Microsoft® ActiveScript configuration.

Ticketing

Most of the sample workflows have tickets configured to be sent to the SampleAudit table in the transaction repository, as an example of how you can create auditing records.

Notifications

Most workflows have notifications configured to send a en email to the provisioner or end user indicating whether the action succeeded or failed. The email is also sent to the master email address configured during the Express Configuration.

Confirmation and Summary

Although the Confirmation form is pre-configured, the confirmation screen is not displayed when the workflow is executed unless the **REQUIRE ACTION CONFIRMATION** checkbox is selected on the Properties form. You configure the Properties form separately for each action within a workflow. For example, you can require confirmation for a delete action but not for an add action. None of the sample workflows have confirmation enabled by default.

The Summary form is configured to display summary status while the action is being processed. You can configure this form so that the summary does not show until the action completes and can choose to hide some of the buttons on the Summary screen. Additionally, you can choose which summary statistics are displayed to the end user.

Unused Forms in the Sample Workflows

The following forms are not used in any of the sample workflows: Seed Community, Seed Refine Search, Role Community, Role Refine Search, Approval Community, Delegation Community, Conditions, Account ID Generation.

Forms Used Only in Specific Workflows

The forms associated with Resource Claiming are used only in the CourionSelfService sample workflow.

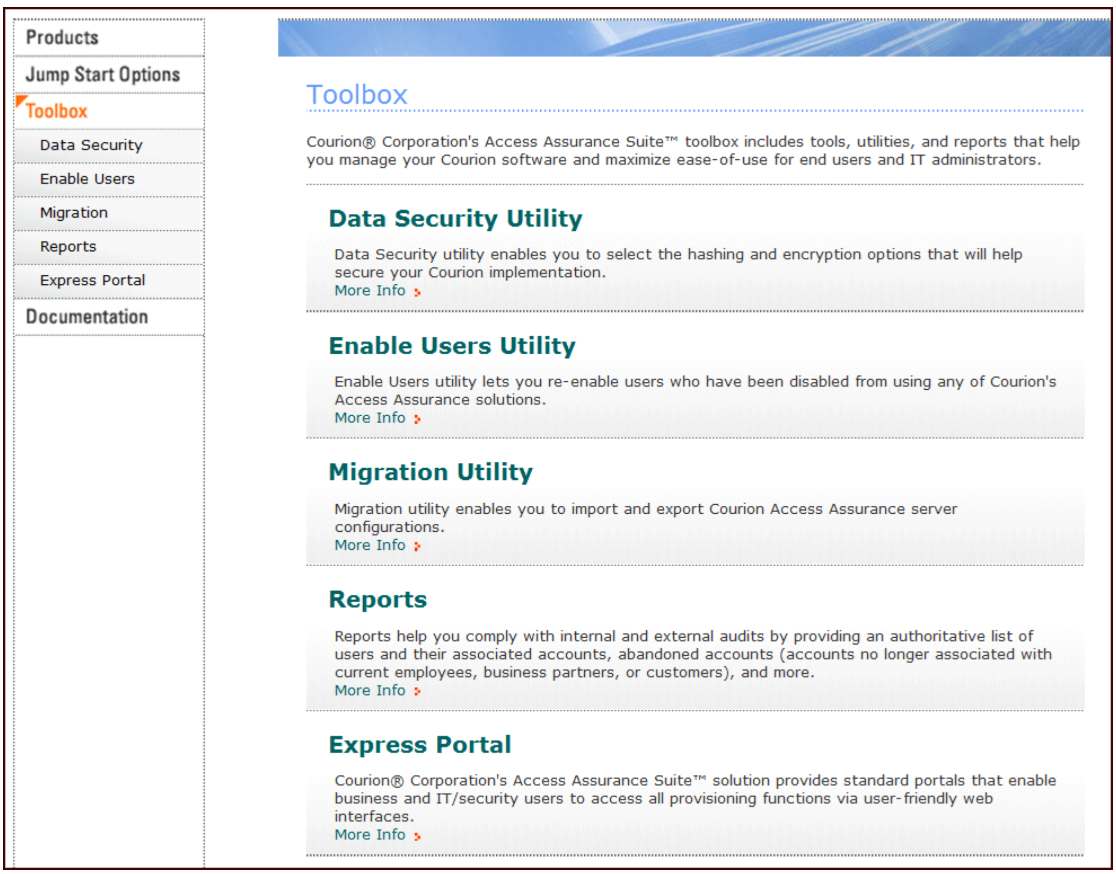
The Mining Refine Search and Mining Community forms are used only in the Core Role Creation and Core Role Management sample workflows.

Chapter 2: Accessing Sample Workflows

You can edit the forms for the sample workflows through Flowchart View or Tree View in the Administration Manager. To run the sample workflows, you access them from the Express Portal in the Access Assurance Suite Console page.

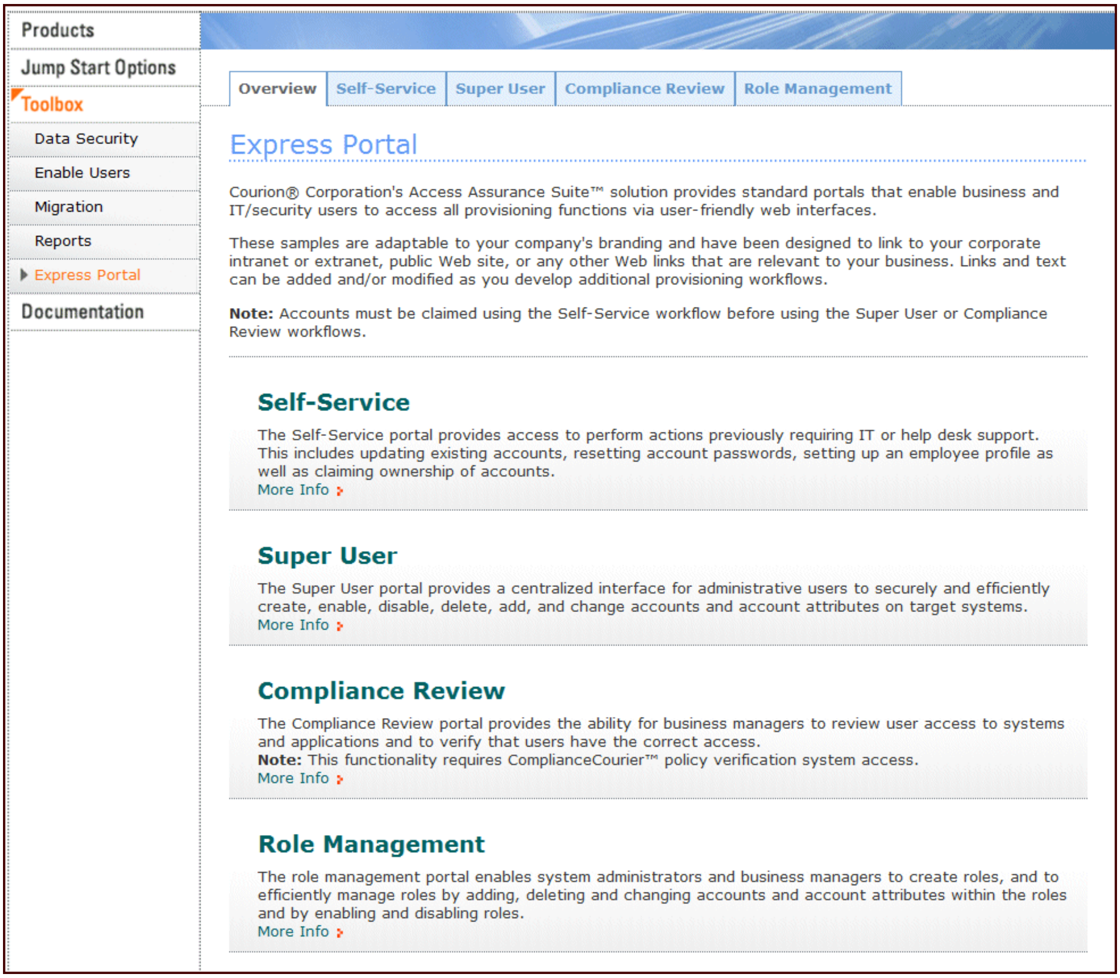
From the Access Assurance Suite console page, expand the Toolbox option on the left side of the page as shown in *Figure 1*.

Figure 1: Selecting the Express Portal



From this page, click on either **EXPRESS PORTAL** from the list of Toolbox options, or **MORE INFO >** at the end of the Express Portal description. The Express Portal page appears, as in *Figure 2*.

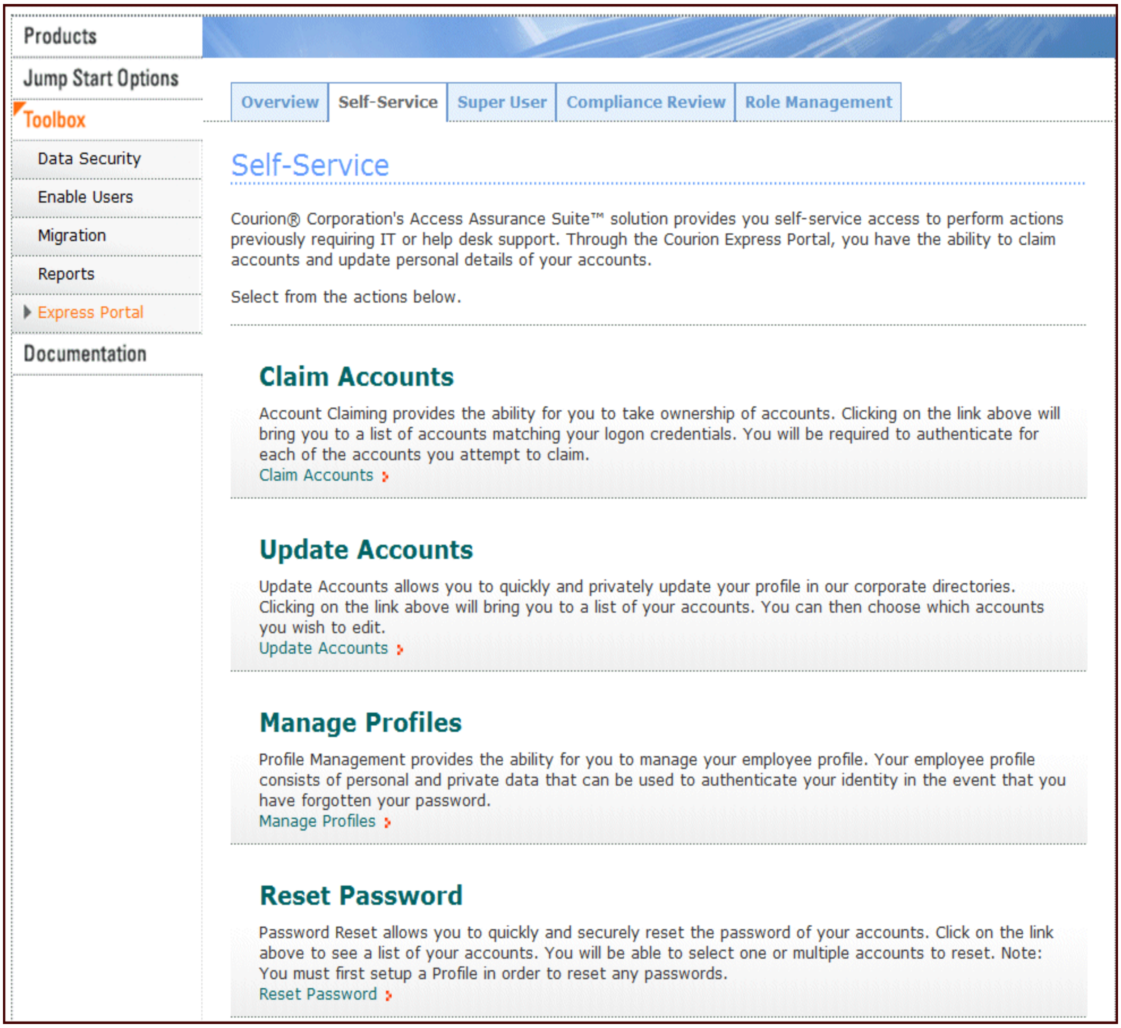
Figure 2: Express Portal Page



From the Express Portal page, you can access workflows by clicking on the appropriate link:

- **SELF-SERVICE** is a link to the portal page for Self-Service workflows, shown in *Figure 3*.
- **COMPLIANCE REVIEW** is a link to the Compliance Review workflow.
- **SUPER USER** is a link to the Super User workflows, shown in *Figure 4*.
- **ROLE MANAGEMENT** is a link to the Role Management workflows, shown in *Figure 5*.

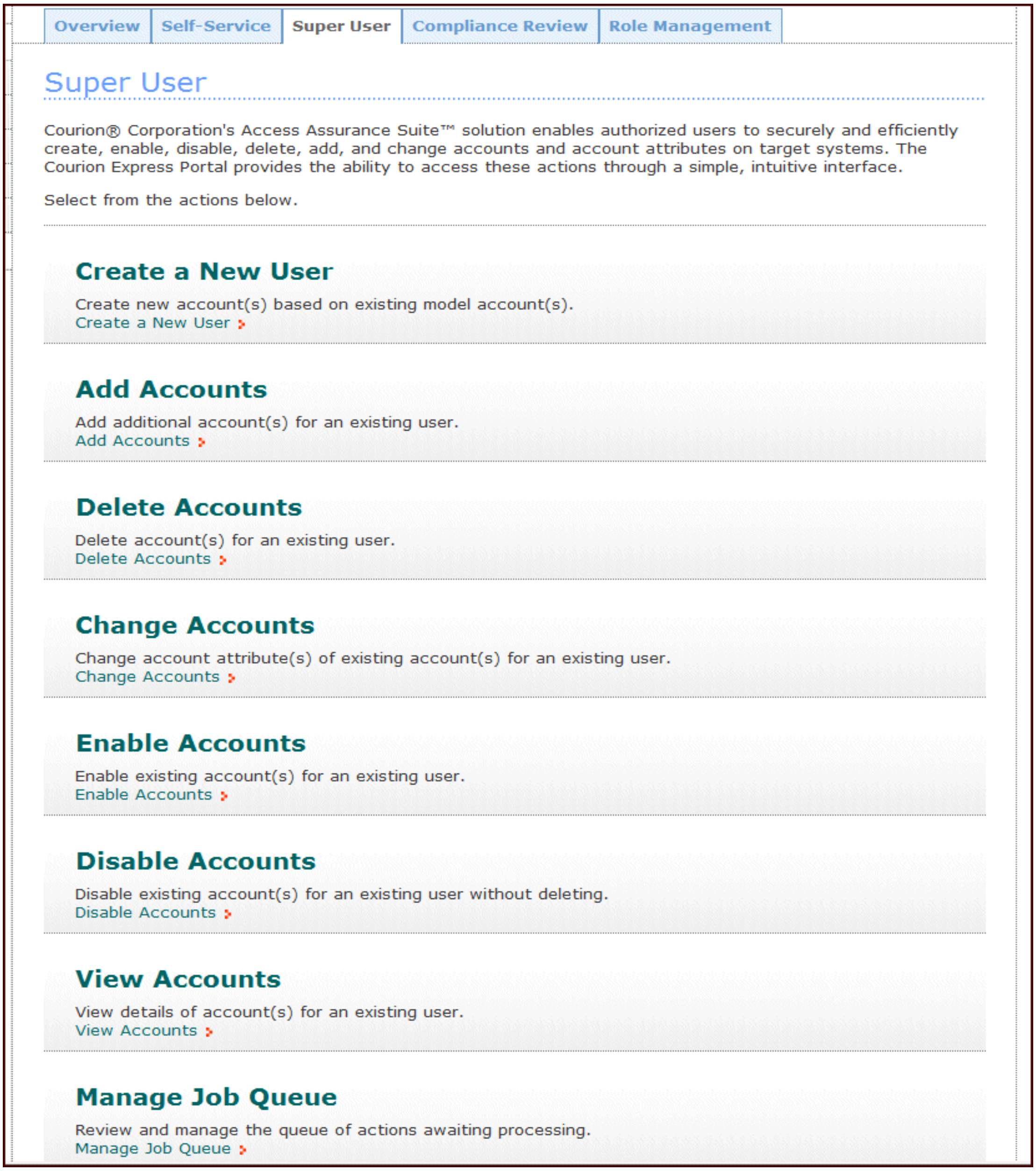
Figure 3: Self-Service Workflow Portal Page



From the Self-Service workflow portal page, you can access workflows by clicking on the appropriate link:

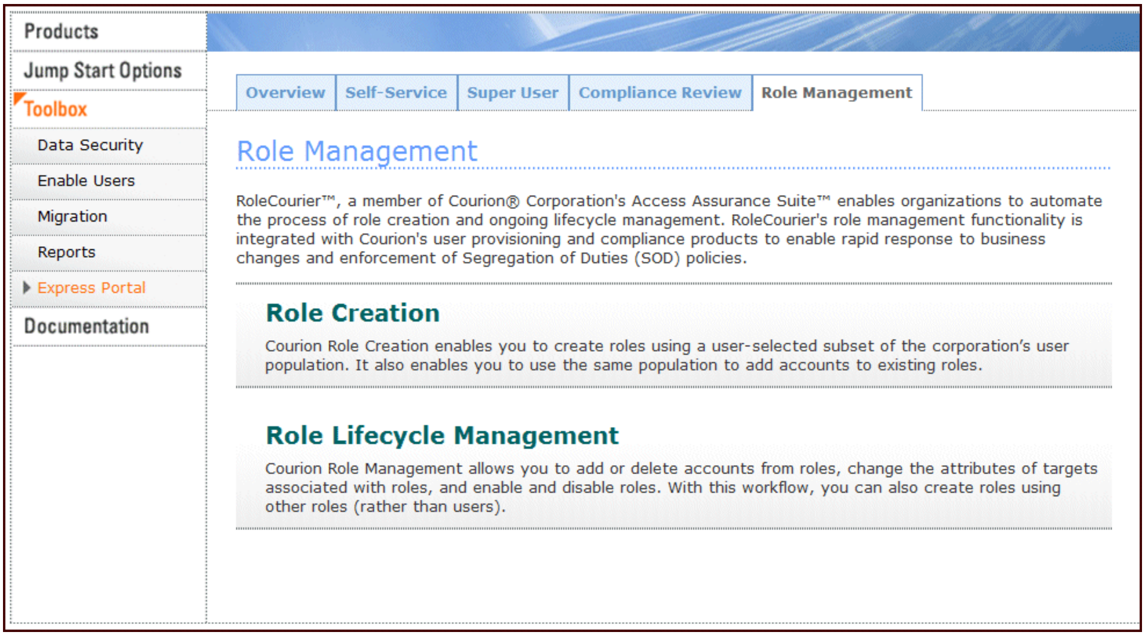
- **CLAIM ACCOUNTS** is a link to CourionSelf-Service using the View action.
- **UPDATE ACCOUNTS** is a link to CourionSelf-Service using the Change action.
- **MANAGE PROFILES** is a link to CourionSelf-Service Profile Management
- **RESET PASSWORD** is a link to CourionSelf-Service Password Reset

Figure 4: Super User Workflow Page



From the Super User workflow portal page, you can access workflows which enable you to create accounts for a new user, add accounts for an existing user, change attributes of existing accounts, and enable, disable, or delete accounts. You can also review and manage the queue of actions awaiting processing.

Figure 5: Role Management Workflow Page



From the Role Management workflow portal page, you can access workflows by clicking on the appropriate link:

- **ROLE CREATION** supports the Create and Add actions. You can create a new role along with linked template accounts, based on account access for a model user. You can also add additional template accounts to an existing role.
- **ROLE LIFECYCLE MANAGEMENT** supports creation of a role based on an existing role as a model, enabling or disabling of a role, changing account attributes of an existing role, or deletion of template accounts linked to a role.

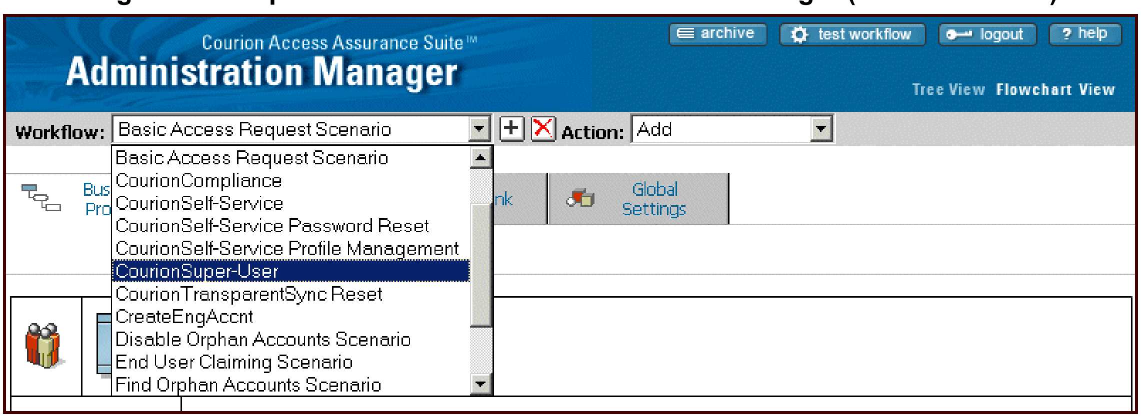
Accessing Administration Manager Forms for Sample Workflows

You can view the Administration Manager forms of each sample workflow from either Tree View or Flowchart View. When you log in to the Administration Manager in Tree View, the sample workflows appear on the left of the screen as in *Figure 6*.

Figure 6: Sample Workflows in the Administration Manager (Tree View)

In Flowchart View, they appear in the Workflow drop-down list, as in *Figure 7*.

Figure 7: Sample Workflows in the Administration Manager (Flowchart View)



Editing Administration Manager Forms for Sample Workflows

Core Security strongly recommends that if you want to edit the configuration settings for a sample workflow, that you create a new workflow by copying the one you want to edit. You can then edit the new workflow while maintaining the original workflow for reference.

Also, if you reinstall the Access Assurance Suite for some reason (such as upgrading to a higher version), you overwrite the preconfigured workflows, including the sample workflows. In this situation, you would lose any edits you made to the sample workflow.

See *"Copying Sample Workflows" on page 241* for information about how to create a workflow by copying an existing workflow.

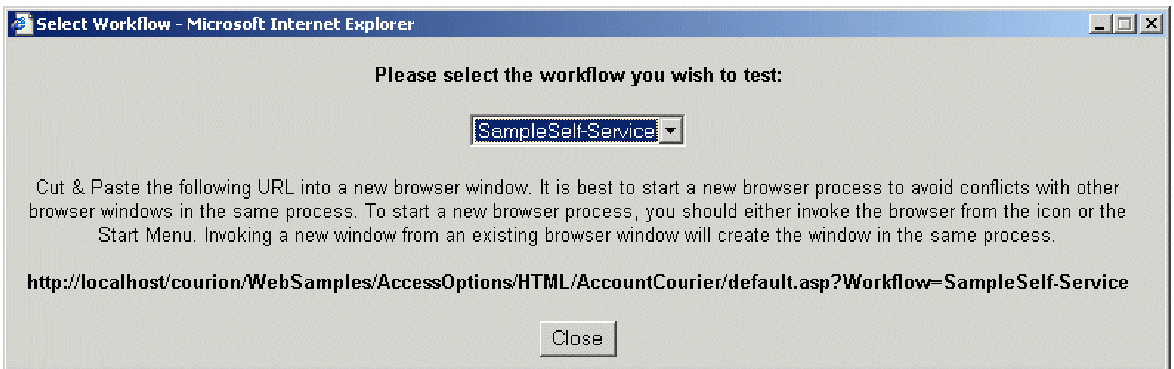
Testing Workflows while in the Administration Manager

You can run the workflow while editing forms in the Administration Manager. To test a workflow, follow these steps:

1. Log in to the Administration Manager (either Tree View or Flowchart View).
2. Click the link **TEST WORKFLOW** button located in on the right side of the Administration Manager header.

   The Administration Manager displays the window shown in *Figure 8*.

Figure 8: Test Workflow Window



3. Select the workflow from the drop-down list.
4. The URL for the selected workflow is automatically copied onto your clipboard. You can then paste the URL into a browser window to run the workflow.

The Administration Manager displays the first authentication step for the workflow you selected.

Chapter 3: Using the Self-Service Claiming Workflow

The Access Assurance Suite uses an IdentityMap datastore to associate user accounts or resources on multiple targets to a specific user. Before you can provision accounts or reset passwords, you need to populate the IdentityMap. In addition to methods such as running a script based account discovery tool, the Courion Self-Service workflow enables end users to claim their own accounts.

When end users run the Self-Service workflow, they authenticate by entering their Active Directory account name and password. The workflow then presents all unclaimed accounts similar to that Active Directory account name. The Self-Service workflow is configured for Active Directory and Exchange only. You need to configure any additional targets in the workflow before those accounts can be claimed.

Users must enter a password for each account they select for claiming. This ensures that users claim accounts belonging to them and prevents users from mistakenly claiming a similarly named account that does not belong to them.

Once an account is claimed, it is available for any provisioning workflow. For a password reset workflow, users also need to create a profile. The Courion Self-Service Profile Management workflow creates and maintains user profiles. For details, see *"Configuring a Profile Management Workflow" on page 27*.

Using the Self-Service Workflow

Follow these steps to use the Self-Service Workflow:

1. From the Access Assurance Suite Administration Console, select **TOOLBOX**, **EXPRESS PORTAL**, and **SELF-SERVICE**. From the Self Service page, select **CLAIM ACCOUNTS**.
2. On the **WELCOME** screen, enter your **ACTIVE DIRECTORY ACCOUNT NAME** and **AD ACCOUNT PASSWORD** and click **NEXT**.
3. The **SELECT ACCOUNTS TO CLAIM** screen lists account names that are similar to your Active Directory account name. Two tables display accounts available to be claimed and accounts which have already been claimed and are known to belong to you. Select the accounts that you want to claim. You need to enter the password for each account that you attempt to claim. Click **NEXT**.
4. The **ACCOUNT CLAIMING AUTHENTICATION** screen displays each Active Directory account you are attempting to claim. Enter the password for each account and click **NEXT**.
5. The **CLAIMING SUMMARY** screen lists the status of your attempt to claim accounts. Click **NEXT**.
6. The **ACCOUNT SUMMARY** screen appears displaying details about each of the accounts you have claimed. Click **NEXT**.

7. The **PROCESS COMPLETE** screen appears. At this point, you can either close the browser window, or click **NEXT ACTION** to be taken to the **ACCOUNT ACTIONS** screen. From this screen, you can click **UPDATE ACCOUNTS** to change specified personal details (such as name, phone number, etc.) for your account.

Chapter 4: Configuring a Profile Management Workflow

The Courion Self-Service Profile Management workflow enables end users to create or maintain a profile, containing information such as an address, phone numbers, email, and other personal authentication data.

To use the Self-Service Password Reset workflow, users need a custom question and answer stored in their profile, so users must run the Self-Service Profile Management workflow before they can run the Self-Service Password Reset workflow.

The sections in this chapter use the Courion Self-Service Profile Management sample workflow, providing practical examples of how to configure ProfileCourier workflows:

- *"Details on Global Settings Specific to the Self-Service Profile Management Workflow" on page 28* describes information specific to this workflow.
- *"Creating a New Profile" on page 29* describes using the Add action in the Self-Service Profile Management workflow to create a profile.
- *"Updating an Existing Profile" on page 38* describes using the Change action in the Self-Service Profile Management workflow to update a profile.

Details on Global Settings Specific to the Self-Service Profile Management Workflow

When the sample workflows are installed during Express Configuration, a number of forms are pre-configured that are not described in this manual. You can modify these forms based on your specific needs. An overview of these forms, applying to all the sample workflows, is described in *“Global Settings” on page 13*.

Additionally, the following information is specific to the Courion Self-Service Profile Management sample workflow:

Transaction Repository

User profiles are stored in the Sample Profile table in the Transaction Repository. Only one profile is stored per user.

Macros

Since only a single profile is allowed per user, there are two custom macros used to prevent a user with an existing profile from selecting the Create option, or a user with no profile from selecting the Update option. The `%GetIDMapRestriction%` macro is assigned as a restriction for the IdentityMap. The `%GetIDMapMessage%` macro returns an error message to the user if the wrong option is selected.

Additionally, for the Create option, there are several macro which are used to retrieve information from the user’s AD account (such as name, address, and phone number) and automatically populate those fields in the user’s profile.

Unused Forms in the Self-Service Password Reset Workflow

The following forms are not used in this workflow: Provisionee Community, Provisionee Refine Search, Role Community, Role Refine Search, Mining Community, Mining Refine Search, Resource Refine Search, IdentityMap Screen, Approval Community, Delegation Community, Resource Claiming, Resource Suggestions, Password Synchronization, Conditions, Account ID Generation.

Creating a New Profile

This section describes how to configure the Add action to create a new profile, using the Courion Self-Service Profile Management sample workflow.

With this workflow, an end user creates a profile record that is stored in the transaction repository. The Self-Service Profile Management workflow enables end users to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select the Create New Profile option
3. Enter their custom question and answer, along with other personal information.

Note: Since only one profile is allowed per user, if a user with an existing profile selects the Create New Profile option, an error message appears, explaining to the user that they must use the Update Profile option.

The following sections describe configuration of the forms needed for the Add action:

- *"Configure Properties for the Add Action" on page 29* determines which forms are presented to the end user.
- *"Define a Resource Community" on page 31* describes how to set up a form that specifies a model profile record on which to base a new profile. A community restriction is used to select a specific profile record named "modelacct".
- *"Specify Unique Resource Data Fields for the Target" on page 33* describes how to set up a form the end user completes that specifies the fields required to add the new profile.

Configure Properties for the Add Action

To modify the Properties for Add Action Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSELF-SERVICE PROFILE MANAGEMENT** (or the new workflow you have created by copying CourionSelf-Service Profile Management) from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **ADD** from the **ACTION** drop-down menu.
4. Click on **ADD REQUEST**.
5. Click on **PROPERTIES**.

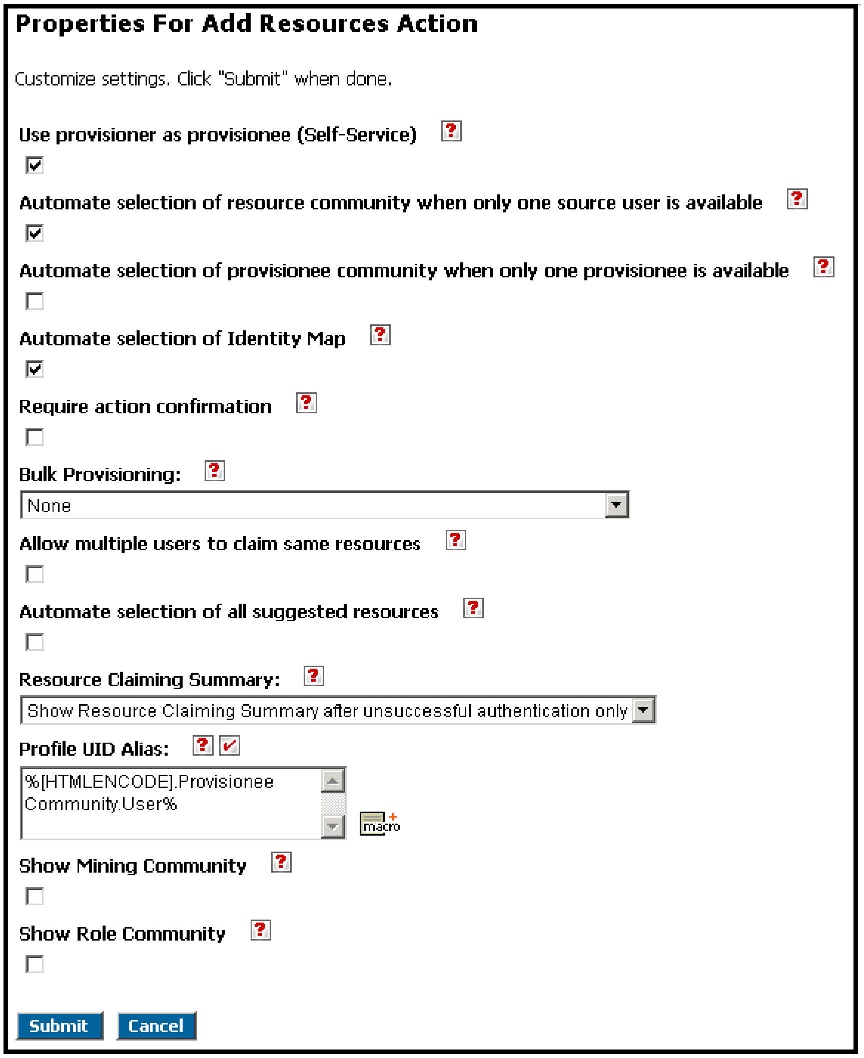
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSELF-SERVICE PROFILE MANAGEMENT** workflow (or the new workflow you have created by copying CourionSelf-Service Profile Management).
3. Expand **ACTIONS** and expand **ADD**.

4. Click the icon next to **PROPERTIES**.

   The Administration Manager displays the Properties for Add Action Form, shown in *Figure 9*.

Figure 9: Properties for Add Action Form



5. Leave the **USE PROVISIONER AS PROVISIONEE USER (SELF-SERVICE)** checkbox selected, since this is a self-service workflow. Selecting this checkbox causes the workflow to bypass the Provisionee Refine Search screen and the Provisionee Community Screen. For this reason, the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox is disabled if this checkbox is selected.

   Note: Because this is a self-service workflow, the selections for Connector, Target, and Object in the Provisionee Community configuration must match exactly the selections for Connector, Target, and Object in one of the Authentication steps. When the selections are the same, the workflow uses the Provisionee Community's configuration of the ProfileUID field to map against the record identified during the Authentication step. If the selections are not the same, the workflow does not follow in Self-Service mode but instead displays the Provisionee Community to the provisioner.

6. Leave the **Automate selection of resource community when only one source user is available** checkbox selected, since a community restriction is used in the Resource Community to select a model profile account as a base profile. For details, see *"Define a Resource Community" on page 31*.
7. Leave the **Automate selection of provisionee community when only one provisionee is available** checkbox unchecked, since it is disabled for this workflow.
8. Leave the **Automate selection of IdentityMap** checkbox selected. Since there is only a single profile to select, automating the selection eliminates an unneeded selection step for the end user (the Select Accounts to Modify screen).
9. Select the **Require action confirmation** checkbox to have the workflow prompt the end user with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.
10. Leave the **Bulk Provisioning** option set to the default of None. This workflow does not use Bulk Provisioning.
11. Leave the **Allow multiple users to claim same resources** and **Automate selection of all suggested resources** checkboxes unchecked since this workflow does not use resource claiming.
12. The **Resource Claiming Summary** option is not used since this workflow does not use resource claiming.
13. **Profile UID Alias** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the Self-Service Profile Management sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
14. Leave the **Show Mining Community** checkbox unselected since this workflow does not use the mining community.
15. Leave the **Show Role Community** checkbox unselected since this workflow does not use the role community.
16. Click **Submit**.

Define a Resource Community

In the Self-Service Profile Management workflow, the Resource Community is used to specify a model profile record on which to base a new profile. A community restriction is used to select a specific profile record named "modelacct". In most situations, you do not need to specify a different model, but the steps to configure the model account are detailed below in case this is necessary.

Note: The Resource Community selection screen does not appear to the end user, since the **Automate selection of resource community when only one source user is available** checkbox on the Properties form is selected.

To modify the Define Resource Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.

2. Select **CourionSelf-Service Profile Management** (or the new workflow you have created by copying CourionSelf-Service Profile Management) from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Resource Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSelf-Service Profile Management** (or the new workflow you have created by copying CourionSelf-Service Profile Management) from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Resource Community**.

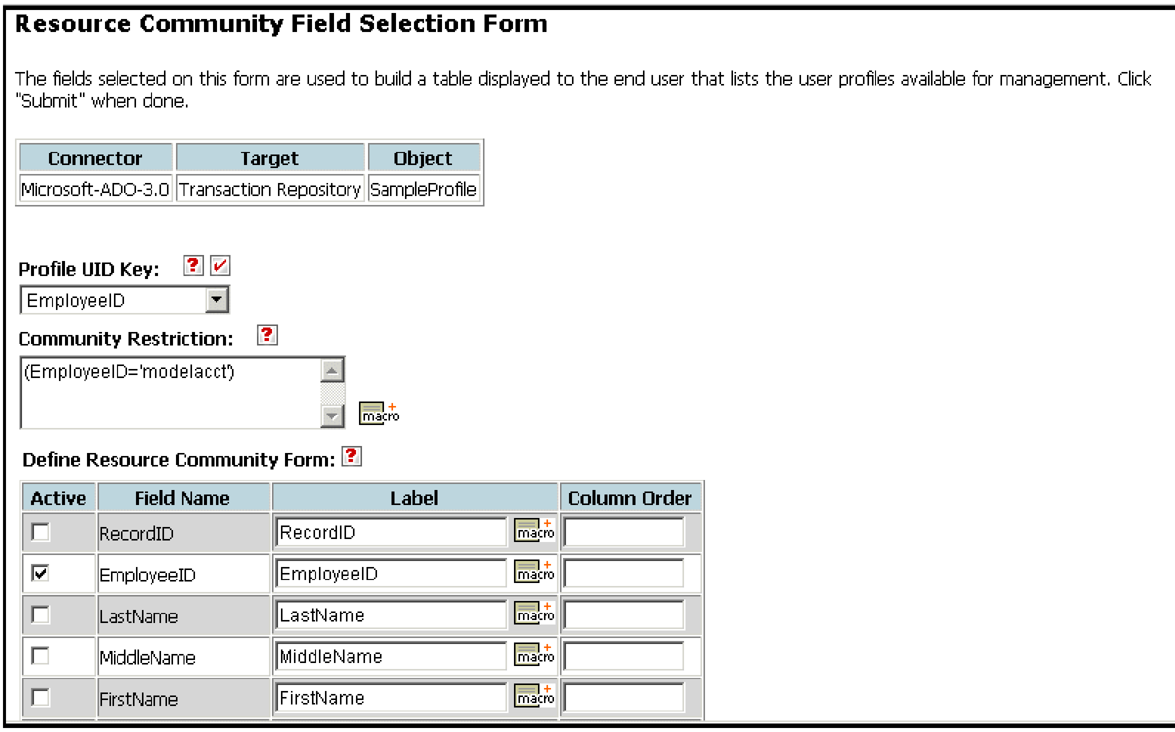
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSelf-Service Profile Management** workflow (or the new workflow you have created by copying CourionSelf-Service Profile Management).
3. Expand **Actions** and expand **Global Settings**.
4. Click the  icon next to **Resource Community**.

You do not need to edit the values in the various text fields on the Resource Community form, since the Resource Community selection screen is not displayed to the end user. Leave the **Select Connector**, **Select Target**, and **Select Object** fields at their default values of Microsoft ADO-3.0, Transaction Repository, and Sample Profile.

5. Click **Configure** to open the Resource Community Field Selection form.

Figure 10: Resource Community Field Selection Form



Resource Community Field Selection Form

The fields selected on this form are used to build a table displayed to the end user that lists the user profiles available for management. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADO-3.0	Transaction Repository	SampleProfile

Profile UID Key:
EmployeeID

Community Restriction:
(EmployeeID='modelacct')

Define Resource Community Form:

Active	Field Name	Label	Column Order
☐	RecordID	RecordID	
☑	EmployeeID	EmployeeID	
☐	LastName	LastName	
☐	MiddleName	MiddleName	
☐	FirstName	FirstName	

6. Leave the **PROFILE UID KEY** set to EmployeeID. This field serves as a link to a user's entries in the Resource Community table.
7. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Statement syntax depends on the target datasource. Do not use hashed or encrypted fields in the statement.

   In the Self-Service Profile Management workflow, the restriction is `EmployeeID='modelacct'`. This selects the model profile that is used a base for creating the new profile.
8. In the Define Resource Community Form table, the only field that needs to be **ACTIVE** is the EmployeeID, since it is used for the **PROFILE UID KEY**.
9. Click **SUBMIT**.

Specify Unique Resource Data Fields for the Target

In the Self-Service Profile Management workflow, the Unique Resource Data form specifies the attributes that can be entered or changed in the user's profile. Several of the attributes are copied into the profile from the user's Active Directory account, but users can change them when creating the profile.

Both the Transaction Repository (used for the profile record) and Active Directory targets have been configured in this workflow. However, only the Transaction Repository/Profile attributes appear to the end user. The Active Directory target is configured here so that various attributes can be copied from the Active Directory account into the profile record automatically.

To automatically populate a specific attribute in the profile, a custom macro is created to retrieve the attribute value from Active Directory and the macro is then assigned as the **Default Value** for that attribute on the Unique Target Data Field Selection Form. As an example, look at the LastName field for the Transaction Repository on this form. For details on how the macro is constructed, you can view the macros on the Modify Custom Macros Form. For details on macros, see *Table 5 on page 245*.

To modify the Unique Target Data Form:

Flowchart View

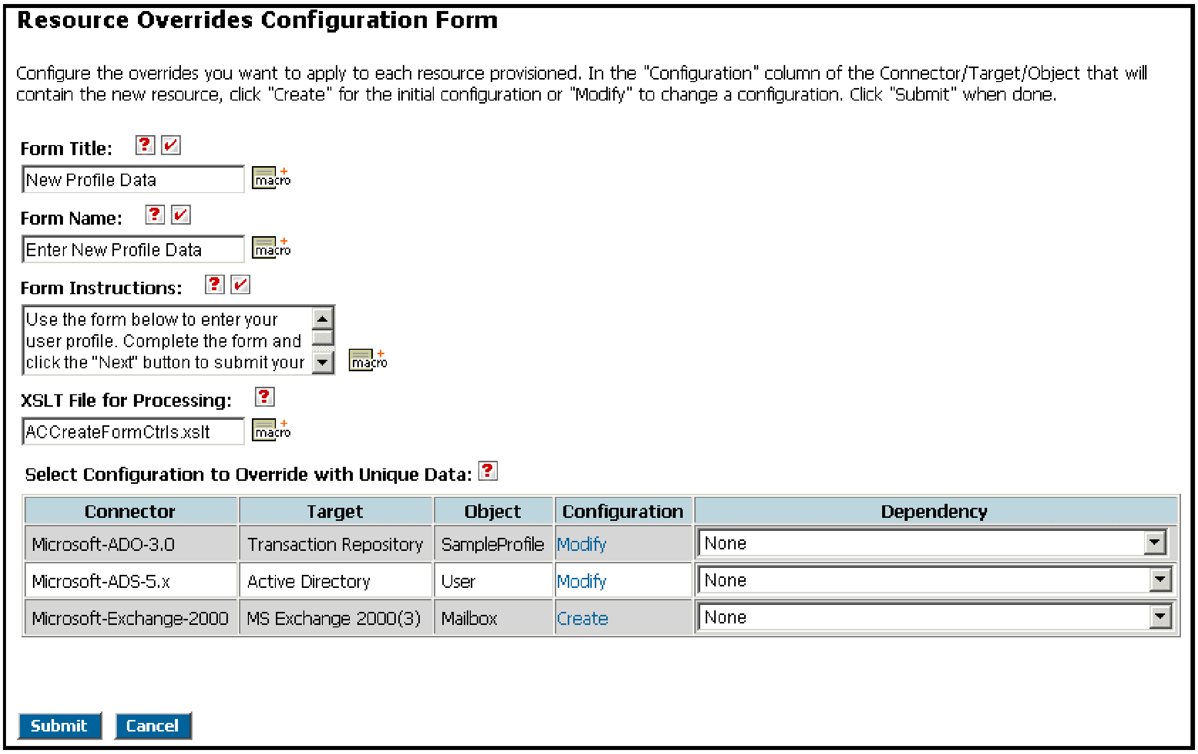
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSelf-Service Profile Management** (or the new workflow you have created by copying CourionSelf-Service Profile Management) from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSelf-Service Profile Management** workflow (or the new workflow you have created by copying CourionSelf-Service Profile Management).
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Unique Resource Data**.

   The Administration Manager displays the Resource Overrides Configuration Form, shown in *Figure 11* with default text and sample data. All text boxes can be edited.

Figure 11: Resource Overrides Configuration Form



Resource Overrides Configuration Form

Configure the overrides you want to apply to each resource provisioned. In the "Configuration" column of the Connector/Target/Object that will contain the new resource, click "Create" for the initial configuration or "Modify" to change a configuration. Click "Submit" when done.

Form Title:
New Profile Data

Form Name:
Enter New Profile Data

Form Instructions:
Use the form below to enter your user profile. Complete the form and click the "Next" button to submit your

XSLT File for Processing:
ACCreateFormCtrls.xslt

Select Configuration to Override with Unique Data:

Connector	Target	Object	Configuration	Dependency
Microsoft-ADO-3.0	Transaction Repository	SampleProfile	Modify	None
Microsoft-ADS-5.x	Active Directory	User	Modify	None
Microsoft-Exchange-2000	MS Exchange 2000(3)	Mailbox	Create	None

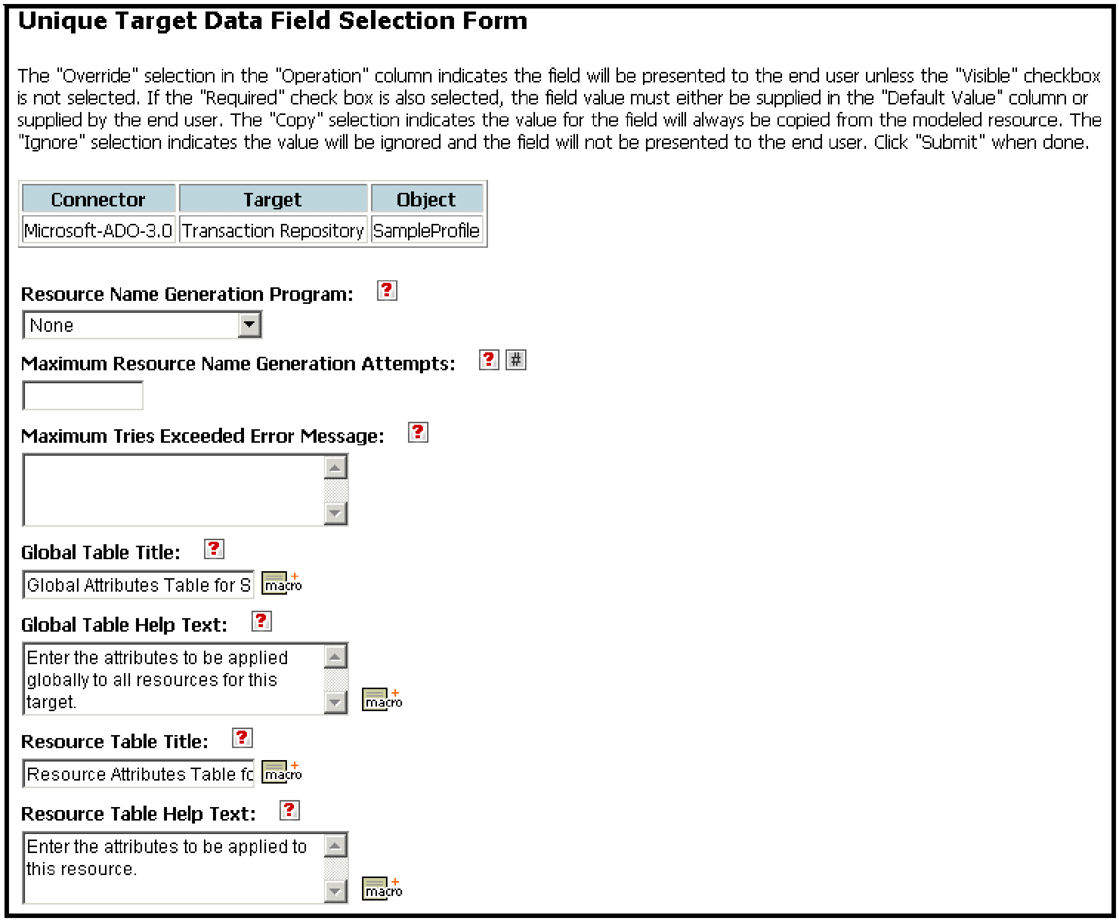
Submit Cancel

5. Text in the **FORM TITLE** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **FORM NAME** text box appears as a title on the form.
7. Text in the **FORM INSTRUCTIONS** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. Specify the file name or a macro that selects the **XSLT FILE FOR PROCESSING**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTLML controls are rendered, controlling how provisioners interact with the data.

   To customize an XSLT file, copy the default file provided by Core Security and rename it. Then edit the renamed file as needed and assign that file to this field.
9. In the **CONFIGURATION** column, click **MODIFY** to change the attribute settings for the Transaction Repository or Active Directory accounts.

The Administration Manager displays the Unique Target Data Field Selection Form (*Figure 12*). The actual content of this form depends on the connector. *Figure 12* shows the top of the form for the Connector for Microsoft ADO (used for the transaction repository).

Figure 12: Unique Target Data Field Selection Form



Unique Target Data Field Selection Form

The "Override" selection in the "Operation" column indicates the field will be presented to the end user unless the "Visible" checkbox is not selected. If the "Required" check box is also selected, the field value must either be supplied in the "Default Value" column or supplied by the end user. The "Copy" selection indicates the value for the field will always be copied from the modeled resource. The "Ignore" selection indicates the value will be ignored and the field will not be presented to the end user. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADO-3.0	Transaction Repository	SampleProfile

Resource Name Generation Program: ?

None

Maximum Resource Name Generation Attempts: ? #

Maximum Tries Exceeded Error Message: ?

Global Table Title: ?

Global Attributes Table for S macro

Global Table Help Text: ?

Enter the attributes to be applied globally to all resources for this target. macro

Resource Table Title: ?

Resource Attributes Table fc macro

Resource Table Help Text: ?

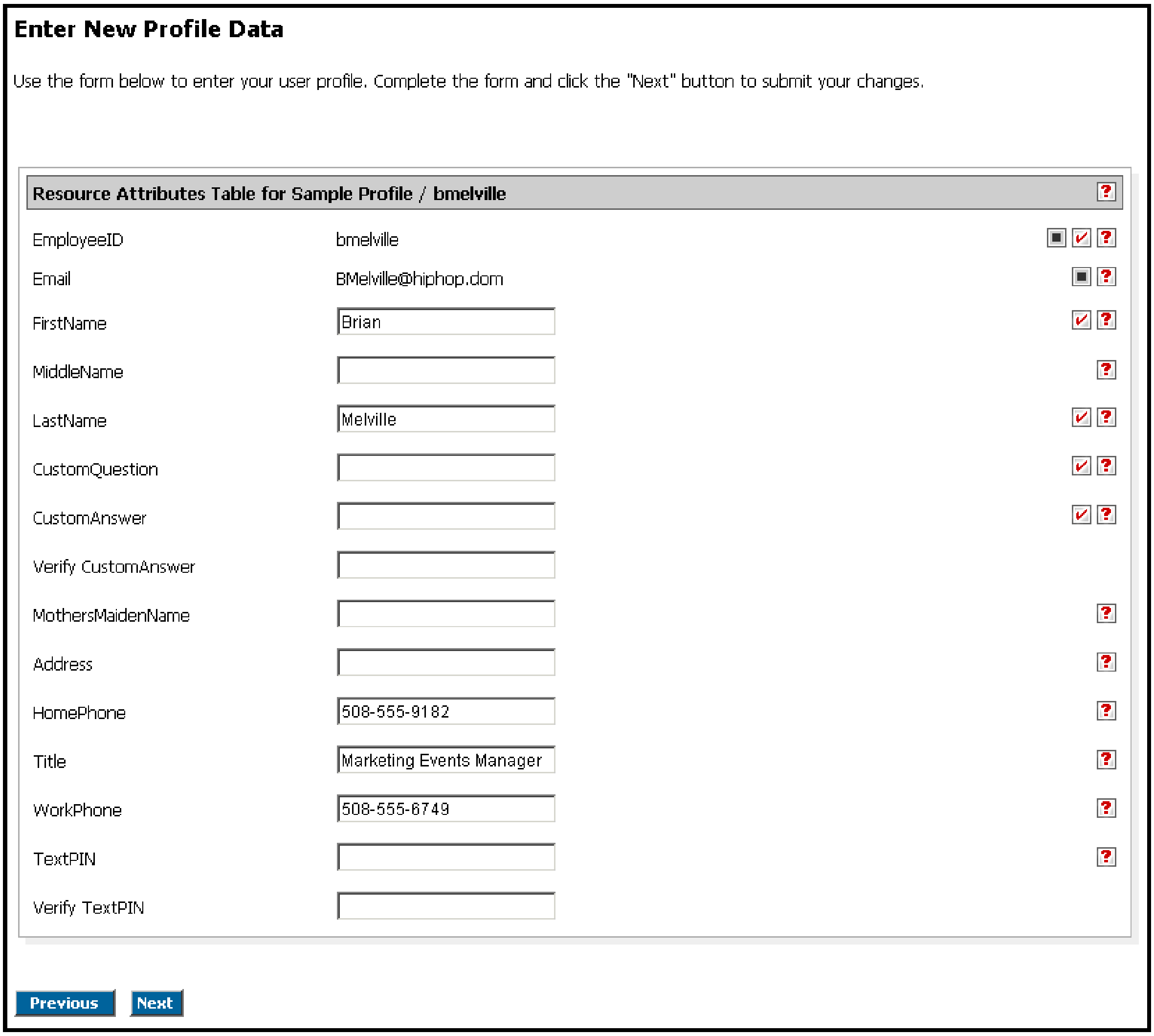
Enter the attributes to be applied to this resource. macro

10. Leave the **RESOURCE NAME GENERATION PROGRAM** set to none, since there is no need to generate a name for the profile.
11. Text in the **GLOBAL TABLE TITLE** text box appears as the heading for the Global Attributes table.
12. Text in the **GLOBAL TABLE HELP TEXT** text box appears as the help for the Global Attributes table.
13. Text in the **RESOURCE TABLE TITLE** text box appears as the heading for each Resource Attributes table.
14. Text in the **RESOURCE TABLE HELP TEXT** text box appears as the help for the Resource Attributes table.
15. Configure the attributes for the target. You can determine whether or not an attribute is exposed to the provisioner, whether it is required, etc. For a description of all fields, see *Table 4 on page 77*.
16. Click **SUBMIT** after completing the Unique Target Data Field Selection Form.

    The Administration Manager redisplays the Resource Overrides Configuration Form (*Figure 11*).

Figure 13 shows the screen displayed to the end user, based on the settings of this form.

Figure 13: Enter a New Profile Screen



Enter New Profile Data

Use the form below to enter your user profile. Complete the form and click the "Next" button to submit your changes.

Resource Attributes Table for Sample Profile / bmelville

EmployeeID	bmelville
Email	BMelville@hiphop.com
FirstName	Brian
MiddleName	
LastName	Melville
CustomQuestion	
CustomAnswer	
Verify CustomAnswer	
MothersMaidenName	
Address	
HomePhone	508-555-9182
Title	Marketing Events Manager
WorkPhone	508-555-6749
TextPIN	
Verify TextPIN	

Previous Next

Updating an Existing Profile

This section describes how to configure the Change action to update a profile, using the Courion Self-Service Profile Management sample workflow.

With this workflow, an end user creates a profile record that is stored in the transaction repository. The Self-Service Profile Management workflow enables end users to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select the Update Profile option
3. Enter their custom question and answer, along with other personal information.

Note: Since only one profile is allowed per user, if a user without a profile selects the Update Profile option, an error message is displayed to the user explaining that they must use the Create New Profile option.

The following sections describe configuration of the forms needed for the Change action:

- *“Configure Properties for the Change Resources Action” on page 38* determines which forms are presented to the end user.
- *“Specify Unique Resource Data Fields for the Target” on page 40* describes how to set up a form the end user completes that specifies the fields required to change the profile.

Configure Properties for the Change Resources Action

To modify the Properties for Change Resources Action Form:

Flowchart View

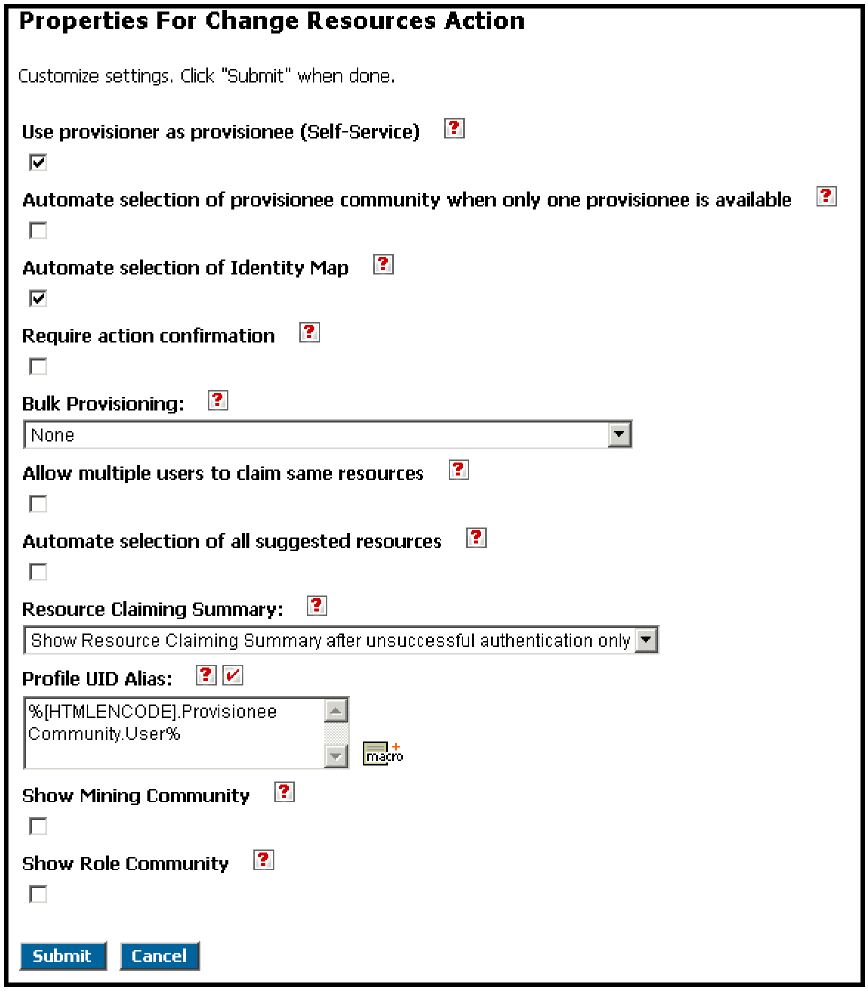
1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSELF-SERVICE PROFILE MANAGEMENT** (or the new workflow you have created by copying CourionSelf-Service Profile Management) from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CHANGE** from the **ACTION** drop-down menu.
4. Click on **CHANGE REQUEST**.
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSELF-SERVICE PROFILE MANAGEMENT** workflow (or the new workflow you have created by copying CourionSelf-Service Profile Management).
3. Expand **ACTIONS** and expand **CHANGE**.
4. Click the icon next to **PROPERTIES**.

The Administration Manager displays the Properties for Change Resources Action Form, shown in *Figure 14*.

Figure 14: Properties for Change Resources Action Form



5. Leave the **USE PROVISIONER AS PROVISIONEE USER (SELF-SERVICE)** checkbox selected, since this is a self-service workflow. Selecting this checkbox causes the workflow to bypass the Provisionee Refine Search screen and the Provisionee Community Screen. For this reason, the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox is disabled if this checkbox is selected.

   Note: Because this is a self-service workflow, the selections for Connector, Target, and Object in the Provisionee Community configuration must match exactly the selections for Connector, Target, and Object in one of the Authentication steps. When the selections are the same, the workflow uses the Provisionee Community's configuration of the ProfileUID field to map against the record identified during the Authentication step. If the selections are not the same, the workflow does not follow in Self-Service mode but instead display the Provisionee Community to the provisioner.

6. Leave the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox unchecked, since it is disabled for this workflow.

7. Leave the **AUTOMATE SELECTION OF IDENTITYMAP** checkbox selected. Since there is only a single profile to be selected, automating the selection eliminates an unneeded selection step for the end user (the Select Accounts to Modify screen).
8. Select the **REQUIRE ACTION CONFIRMATION** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.
9. Leave the **BULK PROVISIONING** option set to the default of None. This workflow does not use Bulk Provisioning.
10. Leave the **ALLOW MULTIPLE USERS TO CLAIM SAME RESOURCES** and **AUTOMATE SELECTION OF ALL SUGGESTED RESOURCES** checkboxes unchecked since this workflow does not use resource claiming.
11. The **RESOURCE CLAIMING SUMMARY** option is not used since this workflow does not use resource claiming.
12. The **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the Self-Service Profile Management sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
13. Leave the **SHOW MINING COMMUNITY** checkbox unselected since this workflow does not use the mining community.
14. Leave the **SHOW ROLE COMMUNITY** checkbox unselected since this workflow does not use the role community.
15. Click **SUBMIT**.

Specify Unique Resource Data Fields for the Target

In the Self-Service Profile Management workflow, the Unique Resource Data form is used to specify the attributes that may be entered or changed in the user's profile.

Both the Transaction Repository (used for the profile record) and Active Directory targets have been configured in this workflow. However, only the Transaction Repository/Profile attributes are displayed to the end user.

In the Change action in the Self-Service Profile Management workflow, all attributes may be edited by the user except the EmployeeID (the Active Directory account name) and Email. Unlike the Add action, there are no macros configured for default values, since it is assumed those attributes were previously populated when the profile was created.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSELF-SERVICE PROFILE MANAGEMENT** (or the new workflow you have created by copying CourionSelf-Service Profile Management) from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CHANGE** from the **ACTION** drop-down menu.
4. Click on **CHANGE REQUEST**.

5. Click on **UNIQUE RESOURCE DATA**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSELF-SERVICE PROFILE MANAGEMENT** workflow (or the new workflow you have created by copying CourionSelf-Service Profile Management).
3. Expand **ACTIONS** and expand **CHANGE**.
4. Click the icon next to **UNIQUE RESOURCE DATA**.

The steps to complete the Unique Target Data Form to change a profile are the same as to create a profile. Follow the instructions provided in *"Specify Unique Resource Data Fields for the Target" on page 33*.

Chapter 5: Configuring a Password Reset Workflow

This chapter describes how to configure a workflow that enables end users to reset their passwords, using the CourionSelf-Service Password Reset workflow as a model. Users do not need to know their current password. Instead, they authenticate by correctly answering the challenge question entered when they created or last updated their profile.

Before end users can use the CourionSelf-Service Password Reset workflow, they must have an entry in the IdentityMap for their accounts, and must use the CourionSelf-Service Profile Management workflow to create a user profile, which includes the custom question and answer. For details on the Profile Management workflow, see *"Configuring a Profile Management Workflow" on page 27*.

If other methods have not been used to populate the IdentityMap, end users can claim their own accounts by using the CourionSelf-Service workflow. For details, see *"Using the Self-Service Claiming Workflow" on page 25*.

The sections in this chapter describe how to configure the Self Service Password Reset workflow:

- *"Details on Global Settings Specific to the Self-Service Password Reset Workflow" on page 42* describes information specific to this workflow.
- *"Forms Used by the Password Reset Workflow" on page 43* describes configuration of the forms used in this workflow.
- *"Configuring a PasswordCourier Support Staff Workflow" on page 56* describes how to configure a workflow that enables support staff to authenticate end users and securely reset passwords on behalf of those end users.

Details on Global Settings Specific to the Self-Service Password Reset Workflow

When the sample workflows are installed during Express Configuration, a number of forms are pre-configured that are not described in this manual. You can modify these forms based on your specific needs. An overview of these forms, applying to all the sample workflows, is described in *"Global Settings" on page 13*.

Additionally, the following information is specific to the Courion Self-Service Password Reset sample workflow:

Target Configuration

The Self-Service Password Reset workflow is configured for only a single target —Active Directory. If you want to reset passwords on additional targets, you need to use the Target Configuration Form within the Global Settings to add those targets.

The Password Reset action uses the PMM Gateway Connector to provide an interface between Password Courier and each PMM. You need to use the Connector Configuration Manager to create new PMM Gateway Connector targets before they can be added in the Target Configuration Form. For details, see the manual *Configuring Connectors and Password Management Modules (PMMs)*.

Macros

The Self-Service Password Reset workflow uses a custom macro, `%GetCustomQuestion%`, to display the custom question that is stored as part of the user's profile.

Unused Forms in the Self-Service Password Reset Workflow

The following forms are not used in this workflow: Role Refine Search, Role Community, Mining Refine Search, Mining Community, Approval Community, Delegation Community, Resource Claiming, Resource Suggestions, Conditions, Account ID Generation.

The Provisionee Refine Search and Provisionee Community forms are configured in the workflow, but these forms are not used in the context of the workflow, because it is a self service workflow. End users are identified and selected when they authenticate into the workflow and the Provisionee Refine Search and Provisionee Community forms are skipped over.

Forms Used by the Password Reset Workflow

With this workflow, end users can reset their Active Directory password without having to know the current password. The Self-Service Password Reset workflow enables end users to:

1. Authenticate by providing their Active Directory account name and answering their custom question correctly.
2. Select the account to reset.
3. Choose a new password for the account.

The following sections describe configuration of the forms needed for the Password Reset action:

- *"Set Up Authentication for the Password Reset Action" on page 43* describes how to set up the two authentication forms required for end user access to a workflow.
- *"Configure Properties for the Password Reset Action" on page 47* determines which forms are presented to the end user.
- *"Define the IdentityMap Screen Form Presentation for the Password Reset Action" on page 50* describes how to set up a form that controls the appearance of the Select Accounts for Password Reset form presented to the end user.
- *"Specify Unique Resource Data" on page 52* describes how to set up a form the end user completes that specifies the fields used for the password reset.

The following instructions describe how to modify the settings in the CourionSelf-Service Password Reset workflow. If you have created a new workflow by copying CourionSelf-Service Password Reset, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Set Up Authentication for the Password Reset Action

Authentication in the CourionSelf-Service Password Reset sample workflow functions differently from authentication in the other sample workflows. Instead of requiring end users to enter an account name and password, users enter an account name and answer the custom question stored in their profile.

There are two Authentication forms, and the process to set up the second one is identical to the first. The only differences between the two forms is in the selection of the information presented to the end user. Authentication **STEP 1** prompts the user to enter an Active Directory account name; Authentication **STEP 2** requires the user answer the custom question. The following screenshots show the forms from Authentication **STEP 2**.

To set up the Properties for Password Reset Action forms:

Flowchart View

You can access the Authentication Form from Flowchart View using either of these methods:

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSELF-SERVICE PASSWORD RESET** from the **WORKFLOW** drop-down menu.

3. Select **Business Process** and **Password Reset** from the **Action** drop-down menu.
4. Click on the icon in the Action request swim lane (for example Add Request).
5. Select **Auth Step 1** or **Auth Step 2** in the Provisioner Community flowchart.

   Note: You can also access the Mining Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSelf-Service Password Reset** from the **Workflow** drop-down menu.
3. Select **Dynamic Communities** from the navigation bar.
4. Click on **Provisioner Community**.
5. Select **Auth Step 1** or **Auth Step 2** in the Provisioner Community flowchart.

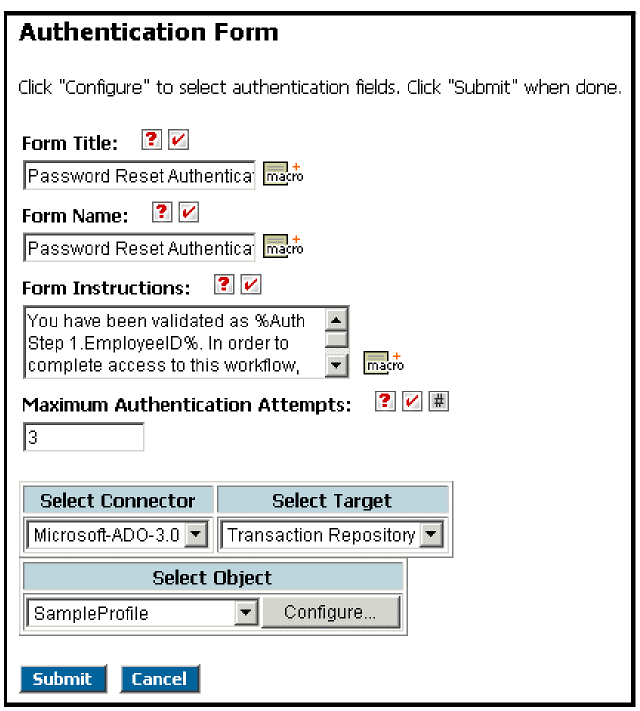
Tree View

1. Log in to the Administration Manager.
2. Expand the **CourionSelf-Service Password Reset** workflow.
3. Expand **Provisioner Community**.
4. Click the icon next to **Step 1** or **Step 2**.

   Note: A third authentication step, **Step 3**, is used for a PasswordCourier Support Staff workflow, and is only available in Tree View.

The Administration Manager displays the Authentication form. The default values for Authentication Step 2 are shown in *Figure 15*.

Figure 15: Authentication Form



5. Text in the **FORM TITLE** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **FORM NAME** text box appears as a title on the authentication form.
7. Text in the **FORM INSTRUCTIONS** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)

   In **STEP 2**, the macro %AuthStep1.EmployeeID% is used to display the Active Directory account name entered by the user in **STEP 1**.
8. In the **MAXIMUM AUTHENTICATION ATTEMPTS** text box, enter the maximum number of failed authentication attempts to allow on this form before disabling the provisioner. The default is 3 attempts.
9. Select a connector from the **SELECT CONNECTOR** drop-down list box.

   Select a target from the **SELECT TARGET** drop-down list box.

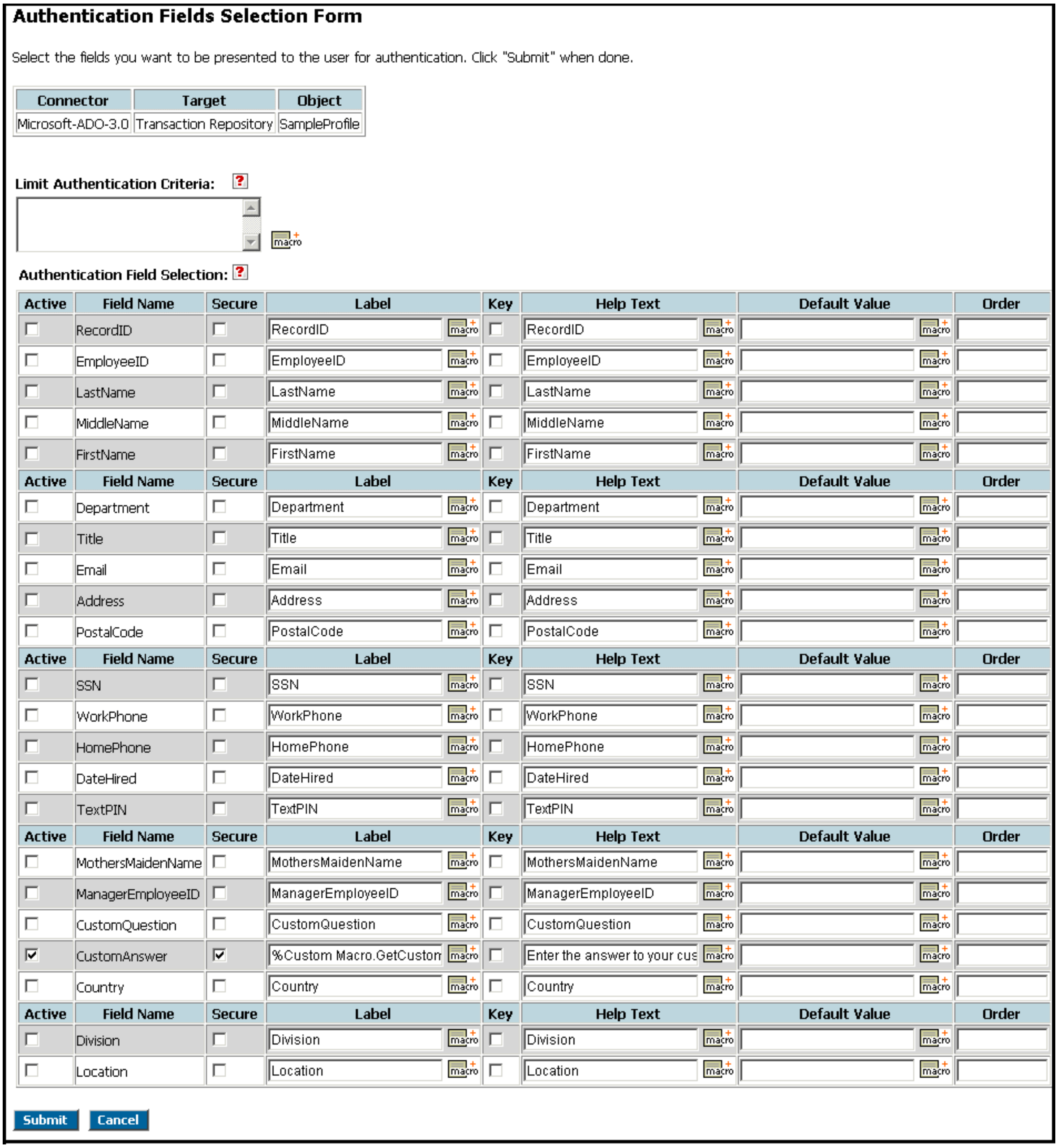
   Select a database table (ODBC target) or object class (LDAP-enabled target) from the **OBJECT** drop-down list box.

   Note: The available connectors and targets depend on what you have added through the Connector Configuration Manager. Collectively, the connector, target, and object identify the datasource against which the provisioner authenticates.

   The Self-Service Password Reset workflow authenticates against the sample profile object stored in the transaction repository (using the connector for Microsoft ADO).
10. Click **CONFIGURE...**.

   The Administration Manager displays the form shown in *Figure 16*. The fields displayed on the forms are examples and depend on the actual object selected.

Figure 16: Authentication Fields Selection Form



Authentication Fields Selection Form

Select the fields you want to be presented to the user for authentication. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADO-3.0	Transaction Repository	SampleProfile

Limit Authentication Criteria:

Authentication Field Selection:

Active	Field Name	Secure	Label	Key	Help Text	Default Value	Order
☐	RecordID	☐	RecordID	☐	RecordID		
☐	EmployeeID	☐	EmployeeID	☐	EmployeeID		
☐	LastName	☐	LastName	☐	LastName		
☐	MiddleName	☐	MiddleName	☐	MiddleName		
☐	FirstName	☐	FirstName	☐	FirstName		
Active	**Field Name**	**Secure**	**Label**	**Key**	**Help Text**	**Default Value**	**Order**
☐	Department	☐	Department	☐	Department		
☐	Title	☐	Title	☐	Title		
☐	Email	☐	Email	☐	Email		
☐	Address	☐	Address	☐	Address		
☐	PostalCode	☐	PostalCode	☐	PostalCode		
Active	**Field Name**	**Secure**	**Label**	**Key**	**Help Text**	**Default Value**	**Order**
☐	SSN	☐	SSN	☐	SSN		
☐	WorkPhone	☐	WorkPhone	☐	WorkPhone		
☐	HomePhone	☐	HomePhone	☐	HomePhone		
☐	DateHired	☐	DateHired	☐	DateHired		
☐	TextPIN	☐	TextPIN	☐	TextPIN		
Active	**Field Name**	**Secure**	**Label**	**Key**	**Help Text**	**Default Value**	**Order**
☐	MothersMaidenName	☐	MothersMaidenName	☐	MothersMaidenName		
☐	ManagerEmployeeID	☐	ManagerEmployeeID	☐	ManagerEmployeeID		
☐	CustomQuestion	☐	CustomQuestion	☐	CustomQuestion		
☑	CustomAnswer	☑	%Custom Macro.GetCustor	☐	Enter the answer to your cus		
☐	Country	☐	Country	☐	Country		
Active	**Field Name**	**Secure**	**Label**	**Key**	**Help Text**	**Default Value**	**Order**
☐	Division	☐	Division	☐	Division		
☐	Location	☐	Location	☐	Location		

Submit Cancel

11. You can use the **LIMIT AUTHENTICATION CRITERIA** to enter a statement to restrict provisioner authentication. However, since this is a self-service workflow, this field is not used.

12. In the **ACTIVE** column, select one or more fields the provisioner must authenticate against. Select at least one field. In the Self-Service Password Reset workflow, the EmployeeID field (which is mapped to the Active Directory account name) is selected in **STEP 1** and the CustomAnswer field is selected in **STEP 2**.

13. In the **SECURE** column, select the field or fields whose input should not be displayed on the form. Secure field input is displayed to the provisioner as a series of asterisks (*****). In **STEP 2** of the Self-Service Password Reset workflow, the CustomAnswer field is marked as Secure.

    Note: It is good practice to mark a field as secure if that field has been marked hashed or encrypted in the Data Security Utility.

14. The **Label** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. In **Step 2** of the Self-Service Password Reset workflow, the label for the CustomAnswer field is a custom macro, `%GetCustomQuestion%`, which displays the end user's custom question.

15. If using two-step authentication, in the **Key** column in **Step 1**, select a field that links field selections in **Step 1** to fields selected in **Step 2**.

    In **Step 1** of the Self-Service Password Reset workflow, the EmployeeID field is selected as the key field.

    (The **Key** column does not apply to **Step 2**, even though it appears on the form.)

16. The **Help Text** column includes default help text for each field name. This text appears when the provisioner hovers the mouse pointer over the help icon for the field on the authentication form. You can edit these fields. The Macro button can also be used to customize the displayed help text.

17. The **Default Value** column is not used in the Self-Service Password Reset workflow, since the user is entering their own information.

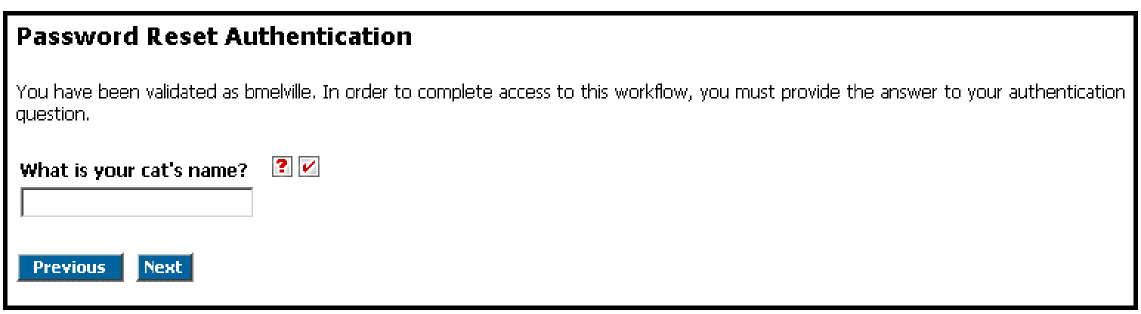
18. In the **Order** column, enter a number for each selected field to determine the order the field names are listed. The field numbered **0** appears at the top of the list. In the Self-Service Password Reset workflow, no order is needed since only one field is selected in each step.

19. The **Datatype** column is informational only and indicates the input field datatype. This information may be useful when constructing help text for a field.

20. Click **Submit** to save selections on the Authentication Fields Selection Form, then click **Submit** on the Authentication Form.

Figure 17 shows the screen displayed to the end-user in **Step 2**, based on the settings from *Figure 16*.

Figure 17: Password Reset Authentication Screen



Configure Properties for the Password Reset Action

To set up the Properties for Password Reset Action form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSelf-Service Password Reset** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Password Reset** from the navigation bar.

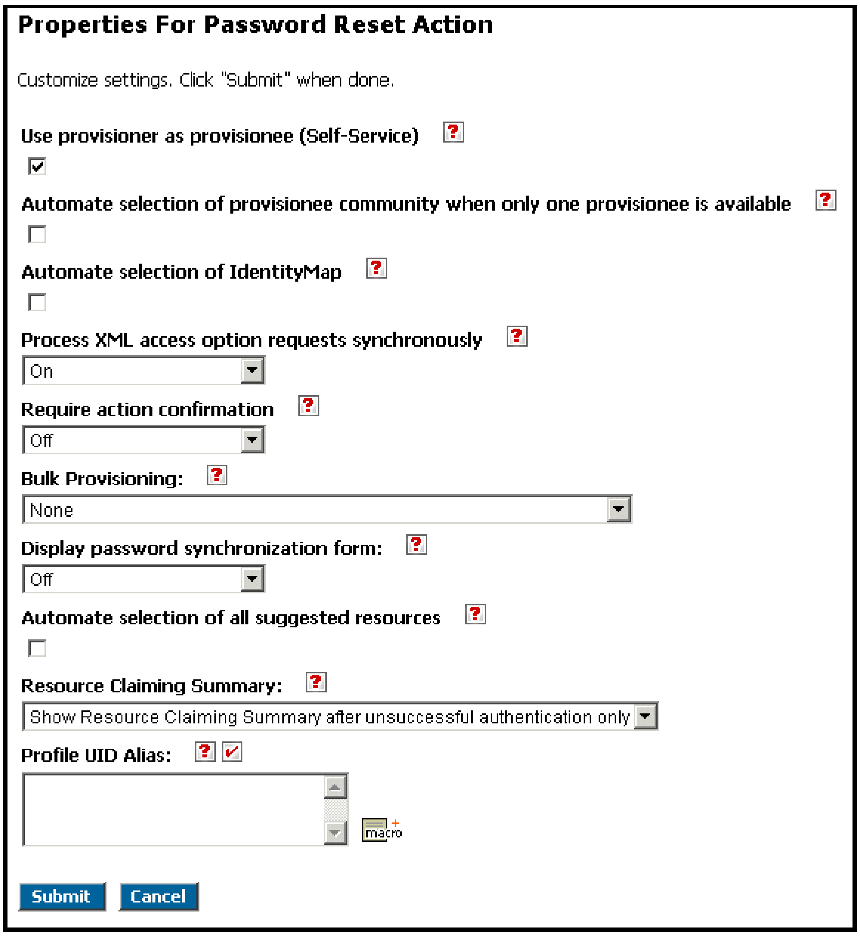
4. Click on **Password Reset Request** and click on **Properties**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSelf-Service Password Reset** workflow.
3. Expand **Actions**, expand **Password Reset**, and expand **Action Settings**.
4. Click the icon next to **Properties**.

   The Administration Manager displays the Properties for Password Reset Action form, shown in *Figure 18*.

Figure 18: Properties for Password Reset Action Form



5. Leave the **Use Provisioner as provisionee user (Self-Service)** checkbox selected, since this is a self-service workflow. Selecting this checkbox causes the workflow to bypass the Provisionee Refine Search screen and the Provisionee Community Screen. For this reason, the **Automate selection of provisionee community when only one provisionee is available** checkbox is disabled if this checkbox is selected.

   Note: Because this is a self-service workflow, the selections for Connector, Target, and Object in the Provisionee Community configuration must match exactly the selections for Connector, Target, and Object in one of the Authentication steps. When the selections are the same, the workflow uses the Provisionee Community's configuration of the ProfileUID field to map against the record identified during the Authentication step. If the selections are not the same, the workflow does not follow in Self-Service mode but instead displays the Provisionee Community to the provisioner.

6. Leave the **Automate selection of provisionee community when only one provisionee is available** checkbox unchecked, since it is disabled for this workflow.

7. The **Automate selection of IdentityMap** checkbox determines whether the Select Accounts for Password Reset screen (showing the end user's accounts) is displayed. If it is unchecked, the accounts are displayed. If it is checked, all of the user's accounts are selected, the Select Accounts for Password Reset screen is skipped, and the workflow proceeds to the Enter New Password screen.

   In the Self-Service Password Reset workflow, the only configured target is Active Directory. If you configure additional targets and plan to use the Password Synchronization feature (to reset multiple passwords at the same time), enable the automatic selection of the Identity Map. This prevents a user from selecting only some of their accounts, thereby causing the passwords to be out of sync.

8. **Process XML access option requests synchronously** — If you are using the XML Access Option for this password reset workflow, this option enables you to specify that you want the password reset action to be processed synchronously so that status can be retrieved. When this option is off, the password reset request is processed asynchronously. The default value is **On**.

   From the drop-down list, select one of the following:

   Force — **Process XML access option requests synchronously** for this workflow is either always on (**On**) or never on (**Off).**

   Conditional — **Process XML access option requests synchronously** for this workflow is enforced when the condition you select evaluates to True. You define conditions with the Create Conditions form. For details, see Table 5 on page 245.

9. Select **Require action confirmation** to have the workflow prompt the provisioner with a confirmation screen. If you do not select this option, the confirmation form does not appear and the workflow skips this step. The default value is **Off**.

   From the drop-down list, select one of the following:

   Force — **Require action confirmation** for this workflow is either always on (**On**) or never on (**Off).**

   Conditional — **Require action confirmation** for this workflow is enforced when the condition you select evaluates to True. You define conditions with the Create Conditions form. For details, see Table 5 on page 245.

10. Leave the **Bulk Provisioning** option set to a value of None. Since this is a self-service workflow, bulk provisioning does not apply.

11. **Display password synchronization form** — The password synchronization form enables users to reset their passwords simultaneously on different targets. See Table 5 on page 245 for information on how to configure Password Synchronization.

    In the Self-Service Password Reset workflow, the only configured target is Active Directory, so password synchronization is not needed and this field is set to a value of **Off**.

12. Leave the **Automate selection of all suggested resources** checkbox unchecked, since Resource Claiming is not used in this workflow.

13. Because Resource Claiming is not used in this workflow, the **Resource Claiming Summary** option is ignored

14. **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. This field is required. The default, used in most of the sample workflows, is `%[HTMLENCODE].Provisionee.Community.User%`.
15. Click **SUBMIT**.

Define the IdentityMap Screen Form Presentation for the Password Reset Action

The settings on the IdentityMap Screen Form determine the formatting of the screen which displays the end user's accounts (as shown in *Figure 20*), enabling the end user to choose which accounts to select.

Note: If the **AUTOMATE SELECTION OF IDENTITYMAP** on the Properties form is enabled, this form is skipped in the workflow, all of the user's accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter New Password screen to the end user).

To define the text on the IdentityMap Form:

Flowchart View

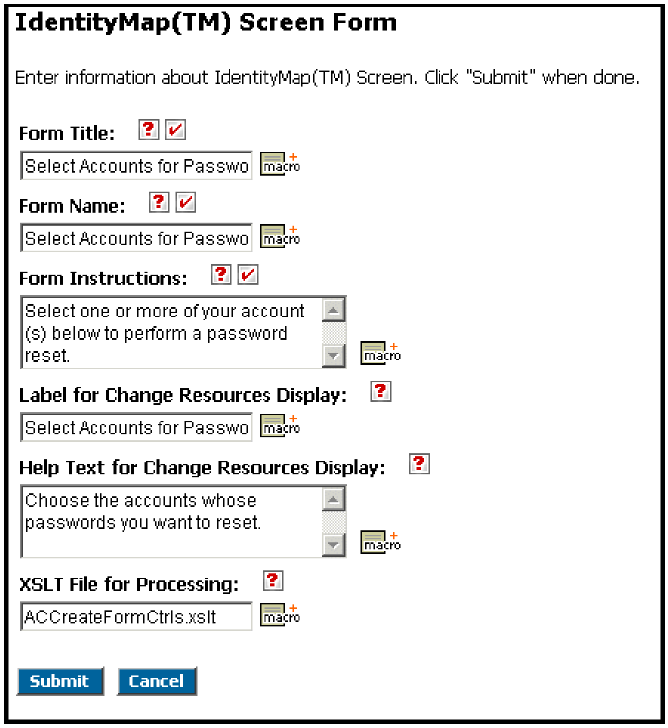
1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSELF-SERVICE PASSWORD RESET** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **PASSWORD RESET** from the navigation bar.
4. Click on **PASSWORD RESET REQUEST** and click on **IDENTITYMAP SCREEN**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSELF-SERVICE PASSWORD RESET** workflow.
3. Expand **ACTIONS**, expand **PASSWORD RESET** and expand **ACTION SETTINGS**.
4. Click the icon next to **IDENTITYMAP SCREEN**.

   The Administration Manager displays the IdentityMap Form for the Password Reset action, shown in *Figure 19* with default text and sample data. All text boxes can be edited.

Figure 19: IdentityMap Screen Form for the Password Reset Action

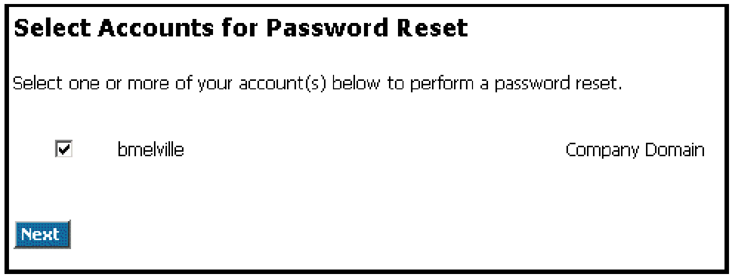


5. Text in the **FORM TITLE** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **FORM NAME** text box appears as a title on the form.
7. Text in the **FORM INSTRUCTIONS** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the "<" and ">" is considered an HTML tag and is not displayed.)
8. Text in the **LABEL FOR CHANGE RESOURCES DISPLAY** text box appears above the list of existing resources associated with the profile.
9. Text in the **HELP TEXT FOR CHANGE RESOURCES DISPLAY** text box describes how to add resources to the selected profile.
10. Specify the file name or a macro that selects the **XSLT FILE FOR PROCESSING**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTML controls are rendered, controlling how provisioners interact with the data.

    To customize an XSLT file, copy the default file provided by Courion and rename it. Then edit the renamed file as needed and assign that file to this field.
11. Click **SUBMIT**.

Figure 20 shows screen displayed to the end user. In the Self-Service Password Reset workflow, the only target configured is Active Directory, so only one account is displayed.

Figure 20: Select Accounts to Reset



Specify Unique Resource Data

You use the Unique Resource Data form to configure which attributes are presented to the end user. In the Self-Service Password Reset workflow, the only attribute presented is the password itself

To set up the Unique Resource Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSelf-Service Password Reset** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Password Reset** from the navigation bar.
4. Click on **Password Reset Request** and click on **Unique Resource Data**.

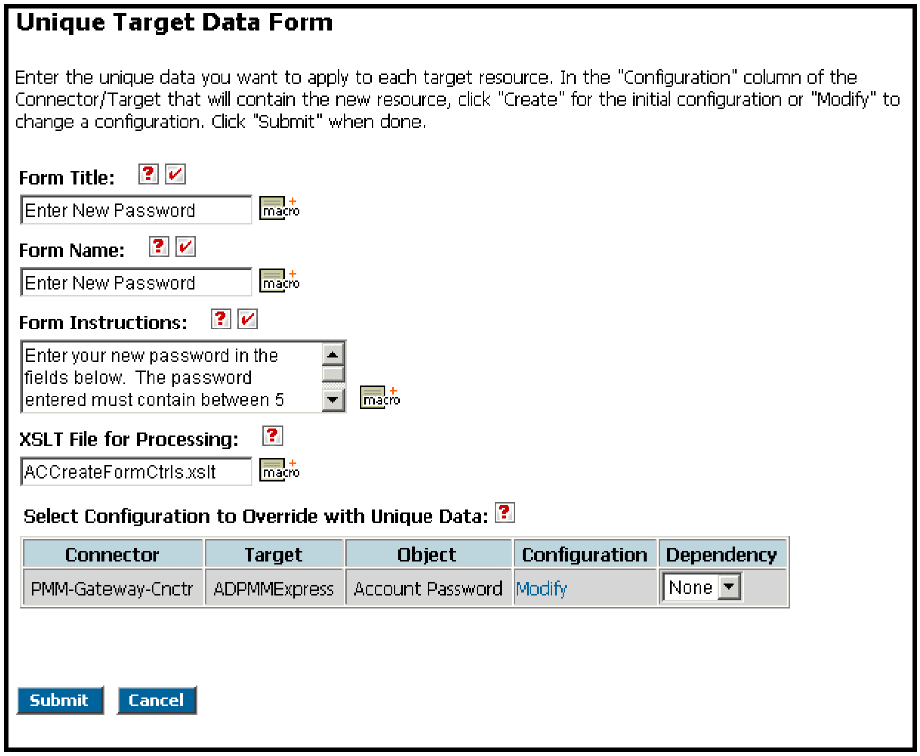
Tree View

1. Log in to the Administration Manager.
2. Expand the **CourionSelf-Service Password Reset** workflow.
3. Expand **Actions**, expand **Password Reset**, and expand **Action Settings**.
4. Click the icon next to **Unique Resource Data**.

   The Administration Manager displays the Unique Target Data Form, shown in *Figure 21*.

In the Self-Service Password Management workflow, only the Active Directory Target is configured. If you want to add additional targets, they must first be added on the Target Configuration Form. For details, see *"Target Configuration" on page 42*.

Figure 21: Unique Target Data Form



Unique Target Data Form

Enter the unique data you want to apply to each target resource. In the "Configuration" column of the Connector/Target that will contain the new resource, click "Create" for the initial configuration or "Modify" to change a configuration. Click "Submit" when done.

Form Title:

Enter New Password

Form Name:

Enter New Password

Form Instructions:

Enter your new password in the fields below. The password entered must contain between 5

XSLT File for Processing:

ACCreateFormCtrls.xslt

Select Configuration to Override with Unique Data:

Connector	Target	Object	Configuration	Dependency
PMM-Gateway-Cnctr	ADPMMExpress	Account Password	Modify	None

Submit Cancel

5. Text in the **FORM TITLE** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **FORM NAME** text box appears as a title on the form.
7. Text in the **FORM INSTRUCTIONS** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. Specify the file name or a macro that selects the **XSLT FILE FOR PROCESSING**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTML controls are rendered, controlling how provisioners interact with the data.

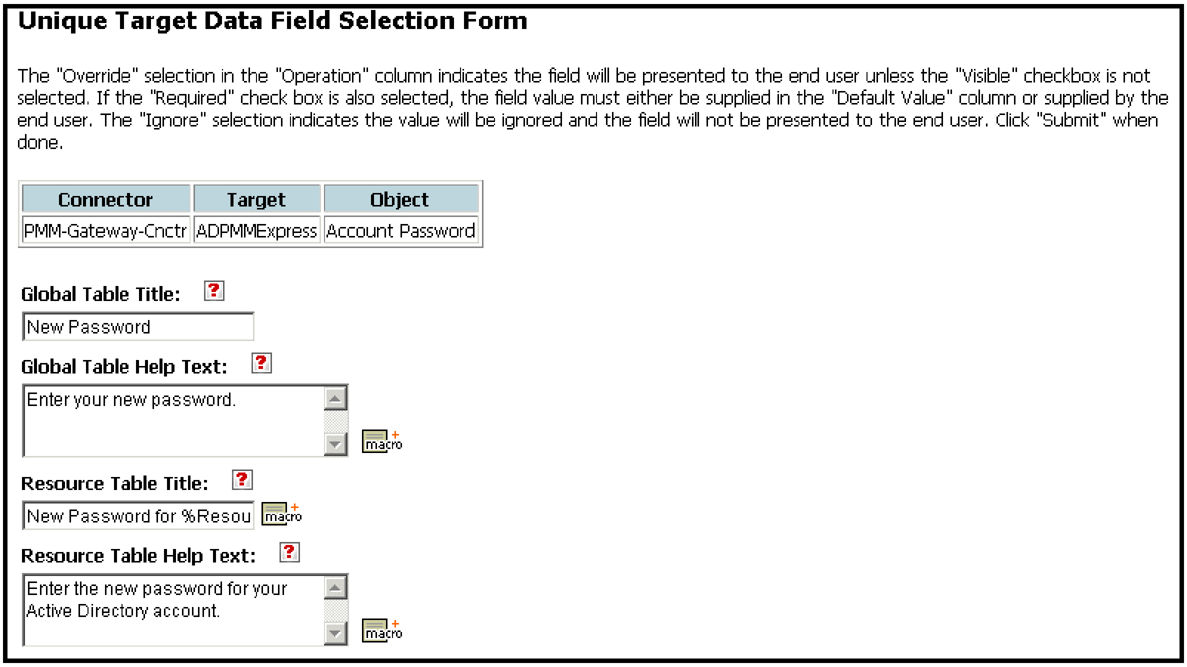
   To customize an XSLT file, copy the default file provided by Courion and rename it. Then edit the renamed file as needed and assign that file to this field.
9. If you have more than one target in the workflow, in the **DEPENDENCY** column, select the name of the target whose password must be successfully reset before any other passwords are reset.

   Note: If you want Target C to be dependent on Target A and Target B, make the following dependency: Target C is dependent on Target B, which is dependent on Target A.
10. In the **CONFIGURATION** column of the connector/target that contains the reset password, click **CREATE**. If a Unique Target Data form for this connector/target has already been configured, click **MODIFY** to change the form.

    The Administration Manager displays the Unique Resource Data Field Selection Form, as in [Figure 22](#).

    The actual content of this form depends on the connector.

Figure 22: Unique Resource Data Field Selection Form



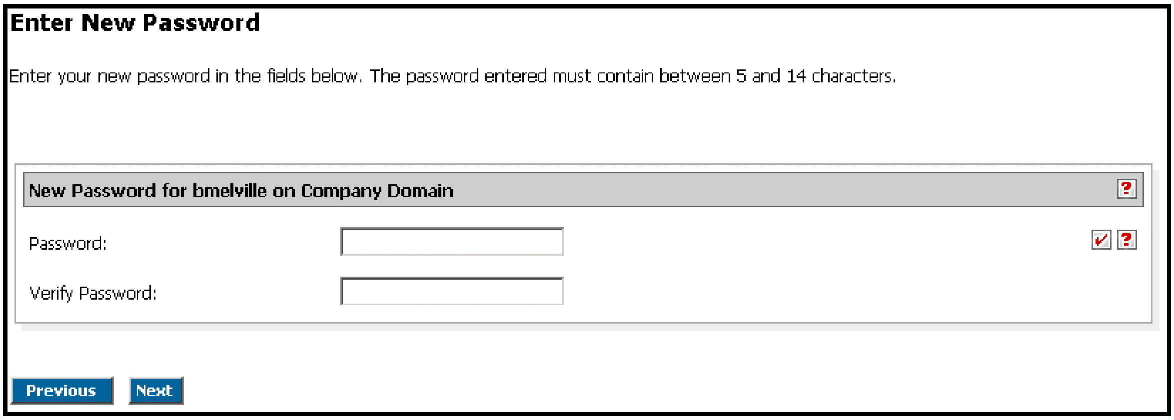
11. Text in the **Global Table Title** text box appears as the heading for the Global Attributes Table.
12. Text in the **Global Table Help** Text text box appears as the help for the Global Attributes table.
13. Text in the **Resource Table Title** text box appears as the heading for each Resource Attributes table.
14. Text in the **Resource Table Help Text** text box appears as the help for the Resource Attributes table.
15. Configure the attributes for the target. You can determine whether or not an attribute is exposed to the end user, whether it is required or secure, etc. For a description of all fields, see *Table 4 on page 77*.

    In the Self-Service Password Reset workflow, only the password attribute is exposed to the end user. For the **Validation** field, the CompanyPwdStrength function has been assigned to this attribute. For details on modifying this function to fit your company’s password strength requirements, see *Table 5 on page 245*.
16. Click **Submit** after completing the Unique Resource Data Field Selection Form.

    The Administration Manager redisplays the Unique Target Data Form (*Figure 21*).
17. Click **Create** or **Modify** to configure a set of attributes for another account or click **Submit** to finish.

Figure 23 shows the screen displayed to the end user, based on the settings of the Unique Target Data Form.

Figure 23: Enter a New Password



Configuring a PasswordCourier Support Staff Workflow

In addition to configuring a Self-Service Password Reset workflow, you can create a workflow that enables support staff to authenticate end users and securely reset passwords on behalf of those end users. The support staff do not require supervisory or administrative privileges on the target system.

This workflow is configured identically to the Self-Service Password reset workflow, with one exception. You need to add a third authentication step.

You can access this third authentication step only from Tree View.

1. Log in to the Administration Manager.
2. Expand the workflow you have created for Support Staff Password Reset.
3. Expand **Provisioner Community**.
4. Click the icon next to **Step 3**.

With three authentication steps, you configure the steps so that the support staff user enters their own account name and password in **Step 1**, the end user account name in **Step 2**, and the end user's custom answer in **Step 3**. Since the first step is used to enter both the account name and password of the support staff user, you need to configure Step 1 so that both the account name and password attributes are selected as in the **Active** column of the Authentication Field Selection table.

For details on configuring the authentication steps, see *“Set Up Authentication for the Password Reset Action” on page 43*.

Chapter 6: Configuring a Super-User Workflow

This chapter describes how to configure a workflow that enables a provisioner to perform a variety of actions on accounts and account attributes, using the CourionSuper-User sample workflow as a model.

The CourionSuper-User workflow includes the following provisioning actions:

- **Create** account for a new user, based on an existing model account
- **Add** additional accounts for an existing user
- **Change** the account attributes of existing accounts
- **Enable** or **Disable** existing accounts
- **Delete** accounts
- **View** user account data

In addition, you can also **Manage the Job Queue** of actions awaiting processing.

The sections in this chapter use the CourionSuper-User sample workflow, providing practical examples of how to configure AccountCourier workflows:

- *"Details on Global Settings Specific to the Super-User Workflow" on page 58* describes information specific to this workflow.
- *"Creating an Account" on page 59* describes configuring the CourionSuper-User sample workflow to create new accounts.
- *"Adding Accounts for an Existing User" on page 81* describes configuring the CourionSuper-User sample workflow to add accounts for an existing user.
- *"Change Attributes for an Existing Account" on page 94* describes configuring the CourionSuper-User sample workflow to change attributes for an existing account.
- *"Disabling and Enabling Accounts" on page 101* describes configuring the CourionSuper-User sample workflow to disable or enable existing accounts.
- *"Deleting Accounts" on page 108* describes configuring the CourionSuper-User sample workflow to delete accounts.
- *"Viewing Account Information" on page 113* describes CourionSuper-User sample workflow to view account attribute information.

Details on Global Settings Specific to the Super-User Workflow

When the sample workflows are installed during Express Configuration, a number of forms are pre-configured that are not described in this manual. You can modify these forms based on your specific needs. An overview of these forms, applying to all the sample workflows, is described in *"Global Settings" on page 13*.

Additionally, the following information is specific to the CourionSuper-User workflow:

Macros

The Super-User workflow uses custom macros which substitute information gathered dynamically by the Courion Server into forms and messages displayed to the end user. Some of the custom macros are used in the Create action, to populate the first and last name in the Active Directory and Exchange accounts with the information entered on the Initial Profile form.

Unused Forms in the Super-User Workflow

The following forms are not used in this workflow: Seed Refine Search, Seed Community, Role Refine Search, Role Community, Mining Refine Search, Mining Community, Approval Community, Delegation Community, Password Synchronization, Resource Claiming, Resource Suggestions, Conditions, Account ID Generation.

Creating an Account

This section describes how to configure the Create action, using the CourionSuper-User sample workflow.

With this workflow, a provisioner creates new Microsoft Active Directory and Microsoft Exchange accounts for a new user, using a model account to set default attribute values. If accounts on additional targets need to be created, you can add them to the workflow. This enables the provisioner to create accounts on all needed targets during the same provisioning action. The Super-User workflow guides provisioners through the following steps:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select a source user as a model for creating the new accounts.
3. Select the accounts that need to be created.
4. Enter initial profile information, such as account name, which is automatically populated into the new accounts.
5. Select individual attributes for each account. Default values for various attributes, based on the model account.

The following sections describe configuration of the forms needed for the Create action:

- *"Configure Properties for the Create Action" on page 60* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Resource Profiles" on page 61* describes how to set up a form the provisioner can complete to filter the resource profiles available in the workflow's community.
- *"Define a Resource Community" on page 63* describes how to set up a form that displays the user profiles available for modeling. The provisioner selects a profile and the provisioning application uses the unique identifier in the profile to search the IdentityMap for all the resources associated with the profile.
- *"Define the IdentityMap Screen Presentation for the Create Action" on page 67* describes how to set up a form that controls the appearance of the Select Resources to Create form presented to the provisioner.
- *"Configure an Initial Profile" on page 68* describes how to set up a form the provisioner completes that specifies the fields required to create a basic profile record for the new Active Directory account.
- *"Specify Unique Resource Data Fields for the Target" on page 74* describes how to set up a form the provisioner completes that specifies the fields, and possible default values, required to create the new accounts.

The following instructions describe how to modify the settings in the CourionSuper-User workflow. If you have created a new workflow by copying CourionSuper-User, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the Create Action

To modify the Properties for Create Action Form:

Flowchart View

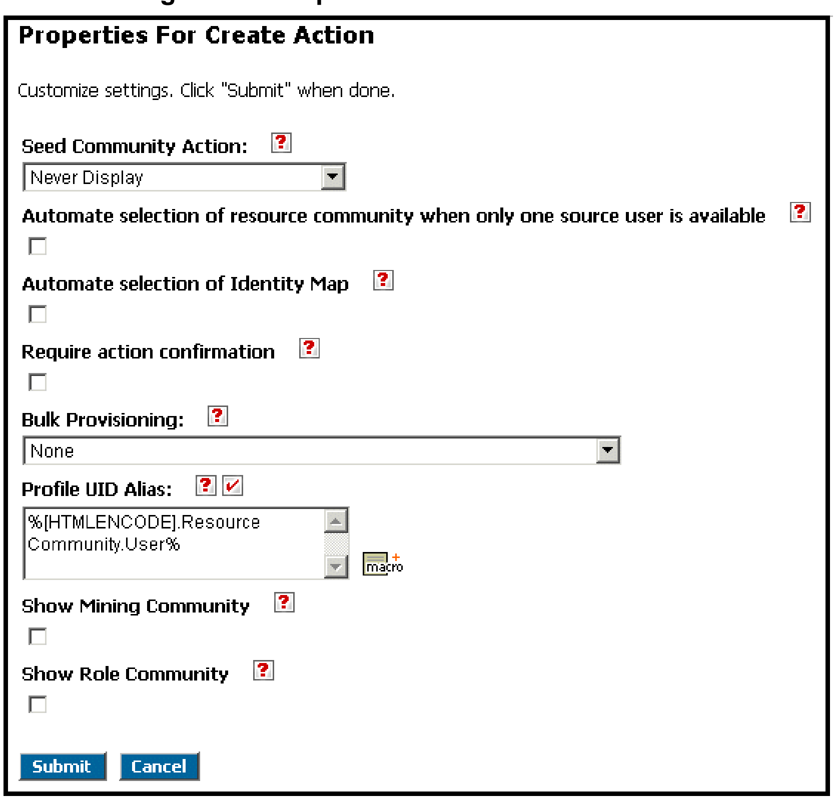
1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CREATE** from the **ACTION** drop-down menu.
4. Click on **CREATE REQUEST**.
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **CREATE**.
4. Click the icon next to **PROPERTIES**.

   The Administration Manager displays the Properties for Create Action Form, shown in *Figure 24*.

Figure 24: Properties for Create Action Form



5. Leave the **SEED COMMUNITY ACTION** option set to the default of Never Display. This workflow does not use the Seed Community.

6. Select the **Automate selection of resource community when only one source user is available** checkbox to enable automatic selection of the source profile (and bypass the Resource Community screen) when only a single source profile is retrieved from the connector. This setting is not selected by default.

   If you have created a special account as a baseline, check this checkbox. If you want the provisioner to be able to choose the baseline from a group of user accounts, leave the checkbox unchecked.

7. Select the **Automate selection of IdentityMap** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **Submit** button. This setting is turned off by default.

   In this workflow, the Resource Community is used to select a user as the baseline. Therefore, if this checkbox is selected, all of the baseline user's accounts are selected and accounts for the new user are created on all those targets.

8. Select the **Require action confirmation** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.

9. Leave the **Bulk Provisioning** option set to the default of None. This workflow does not use Bulk Provisioning.

10. The **Profile UID Alias** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the CourionSuper-User sample workflow, this is set to%[HTMLENCODE].Resource Community.User%.

11. Leave the **Show Mining Community** checkbox unselected since this workflow does not use the mining community.

12. Leave the **Show Role Community** checkbox unselected since this workflow does not use the role community.

13. Click **Submit**.

Refine the List of Displayed Resource Profiles

The CourionSuper-User sample workflow uses the Resource Community to select a baseline user account as a model for creating the a new account.

By default, AccountCourier displays all the users to the provisioner that meet the criteria configured in the Define Resource Community Form. If the filtering criteria for the Define Resource Community Form are broad or the company is large, the community of users could be extensive. You can select one or more fields to include on a Resource Refine Search Form. These fields are presented to the provisioner on the Model User Search screen (*Figure 25*). The provisioner enters values for one or more fields and AccountCourier searches the community and returns a list of users that meet the Resource Refine Search criteria. The provisioner then selects a user from the list as a model.

The provisioner can choose to skip entering data on the Model User Search screen. If the screen is skipped, AccountCourier returns all the user profiles established by the Define Resource Community Form. You may also configure Resource Refine Search Form so that the Model User Search screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Resource Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Resource Refine Search**.

Tree View

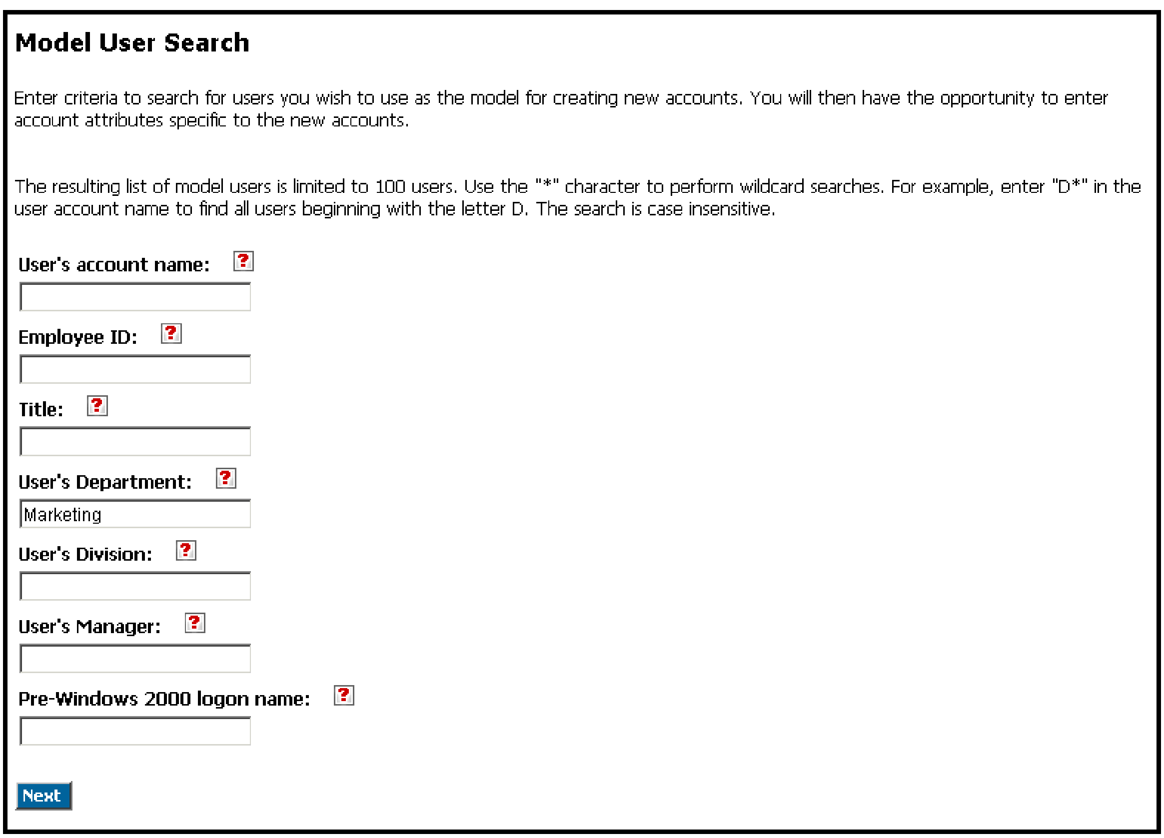
1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the icon next to **Resource Refine Search**.

The process to refine the list of displayed profiles from a Resource Community in the Create action of the Super-User workflow is the same as for a Create action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Figure 25 shows the screen displayed to provisioner, based on the settings from the Super-User workflow.

Figure 25: Model User Search Screen



Define a Resource Community

The CourionSuper-User sample workflow uses the Resource Community to select a baseline user as a model for creating accounts. It is important to choose a baseline user that has all the target accounts that you want to create, since additional targets can not be added in the workflow. (You can, however, use the Add Accounts action in the workflow to add additional targets. See *"Adding Accounts for an Existing User" on page 81* for details.)

By using the Community Restriction parameter, found on the Resource Community Field Selection Form, you can restrict the resources that the provisioner can access. For example, you can set up a list that includes only the members of the Marketing department and restrict the provisioner to only provisioning resources associated with those members of the Marketing department.

In practice, the Community Restriction parameter is often used to select a single baseline user. This ensures that all necessary targets are available for the new user. In this case, you can select the **Automate selection of resource community when only one source user is available** checkbox on the Properties Form, to enable automatic selection of the source profile (and bypass both the Resource Community and resource Refine Search screens).

Note: The Resource Community is global and affects all actions within a workflow. Therefore, any changes made apply to all actions in the Super-User workflow.

To modify the Define Resource Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Resource Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

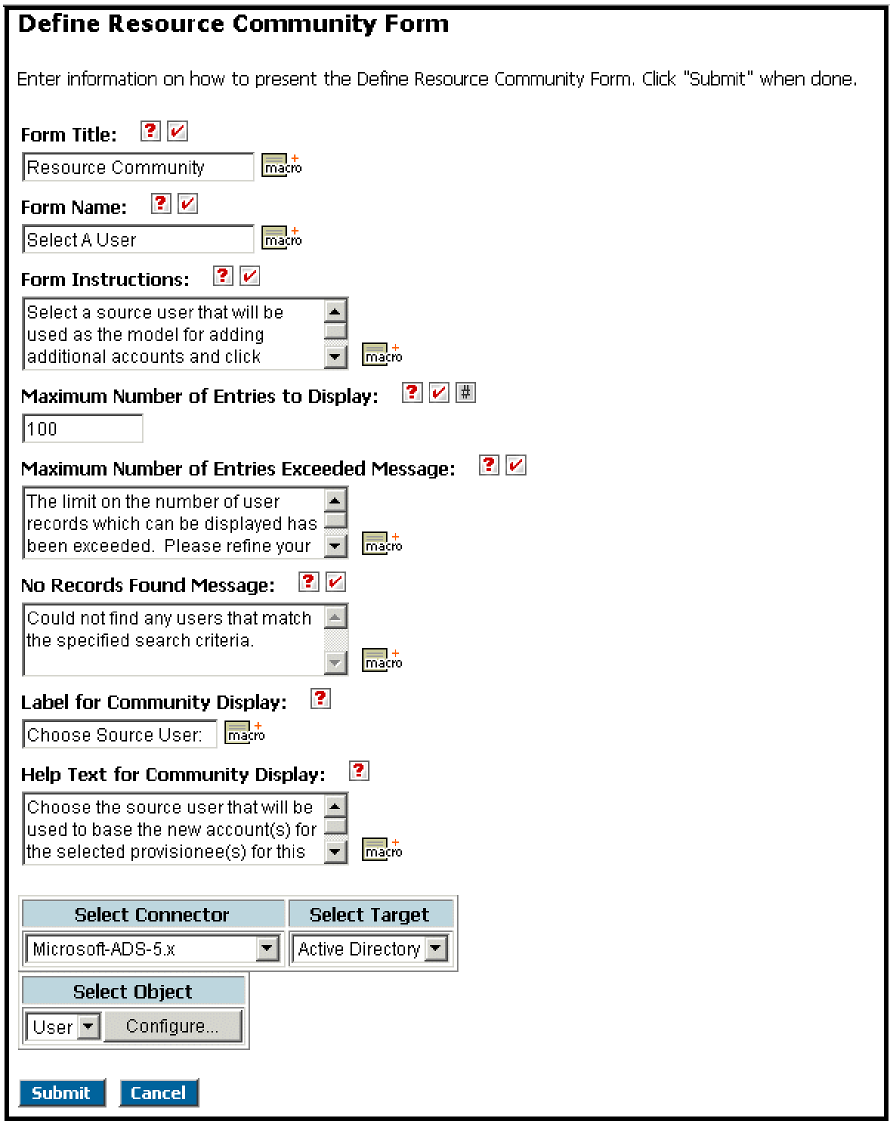
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Resource Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Resource Community**.

The Administration Manager displays the Define Resource Community Form, shown in *Figure 26* with default text and sample data. All text boxes can be edited.

Figure 26: Define Resource Community Form



5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.
7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Source Refine List Form, can help the provisioner limit the number of returned profiles (see *“Refine the List of Displayed Resource Profiles” on page 61*).
9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Source Refine Search Form to display profiles that more closely match search criteria.

10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message displays if the provisioner has entered values on the Source Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label for Community Display** text box appears as a title over the Resource Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Select a connector from the **Select Connector** drop-down list box. In the sample workflow, this is the Connector for Microsoft Active Directory.

    Select a target from the **Select Target** drop-down list box.

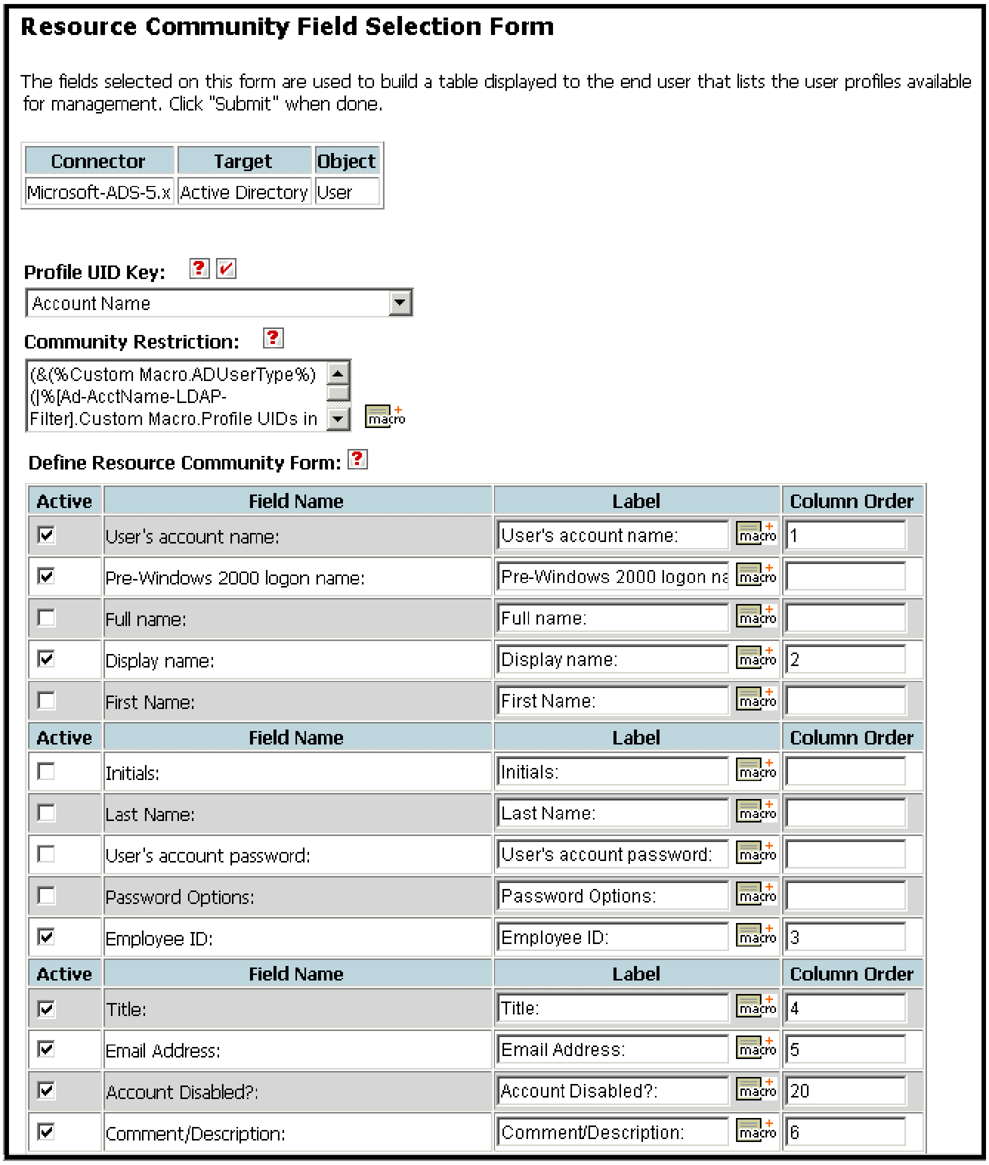
    Select an object from the **Object** drop-down list box.

    Note: The available connectors and targets depend on what has been provided through the Connector Configuration Manager. Collectively, the connector, target, and object point to the datasource that contains the user profiles available in this workflow.
14. Click **Configure...**.

    The Administration Manager displays the Resource Community Field Selection Form, shown in *Figure 27*.

    Note: The fields displayed on the form depend on the object selected. The list of fields has been shortened to save space.

Figure 27: Resource Community Field Selection Form



Resource Community Field Selection Form

The fields selected on this form are used to build a table displayed to the end user that lists the user profiles available for management. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADS-5.x	Active Directory	User

Profile UID Key:

Account Name

Community Restriction:

(&(%Custom Macro.ADUserType%)
(|%[Ad-AcctName-LDAP-
Filter].Custom Macro.Profile UIDs in

Define Resource Community Form:

Active	Field Name	Label	Column Order
☑	User's account name:	User's account name:	1
☑	Pre-Windows 2000 logon name:	Pre-Windows 2000 logon na	
☐	Full name:	Full name:	
☑	Display name:	Display name:	2
☐	First Name:	First Name:	
Active	**Field Name**	**Label**	**Column Order**
☐	Initials:	Initials:	
☐	Last Name:	Last Name:	
☐	User's account password:	User's account password:	
☐	Password Options:	Password Options:	
☑	Employee ID:	Employee ID:	3
Active	**Field Name**	**Label**	**Column Order**
☑	Title:	Title:	4
☑	Email Address:	Email Address:	5
☑	Account Disabled?:	Account Disabled?:	20
☑	Comment/Description:	Comment/Description:	6

15. In the **PROFILE UID KEY** drop-down box, select the unique user ID field in this object that serves as a link to a user's entries, identified by the Profile UID field, in the Resource Community table.

16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Do not use hashed or encrypted fields in the statement.

    In the Super-User workflow, the macro restricts return of available profiles to Active Directory records that belong to users, and only those users with a profile stored in the IdentityMap.

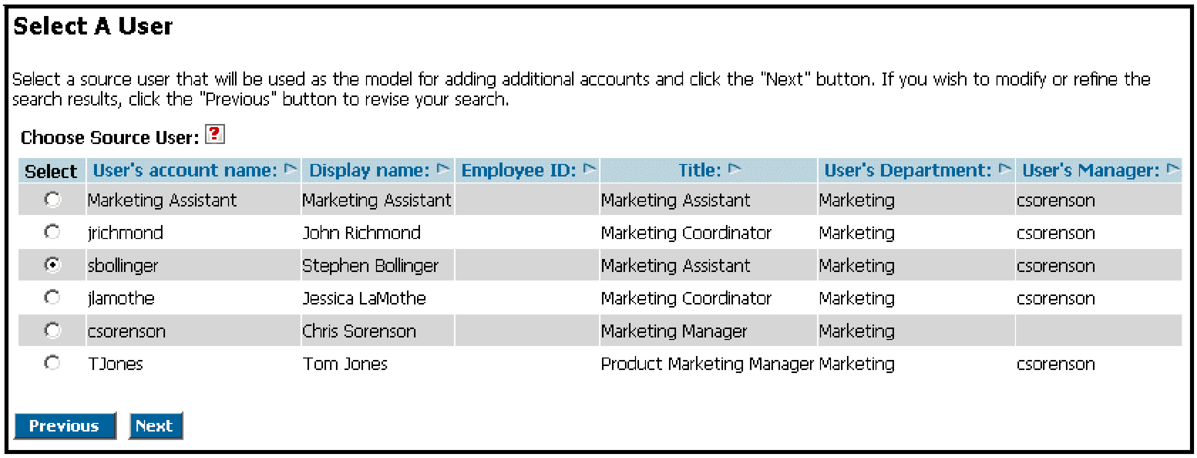
    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on this information.

17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change "EmployeeBadgeNumber" field to "Badge number:".

18. In the **COLUMN ORDER** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered “1” appears as the first column.
19. Click **SUBMIT**.

Figure 28 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 28: Select User Screen



Define the IdentityMap Screen Presentation for the Create Action

The IdentityMap Screen form controls the labels and formatting for the Select Resources to Create screen, shown in *Figure 29*.

Note: If the **AUTOMATE SELECTION OF IDENTITYMAP** on the Properties form is enabled, this form is skipped in the workflow, all of the baseline user’s accounts are selected, and the workflow proceeds to Unique Resource Data form (used to display the Enter Account Information screen to the provisioner).

To modify the IdentityMap Screen Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CREATE** from the **ACTION** drop-down menu.
4. Click on **CREATE REQUEST**.
5. Click on **IDENTITYMAP SCREEN**.

Tree View

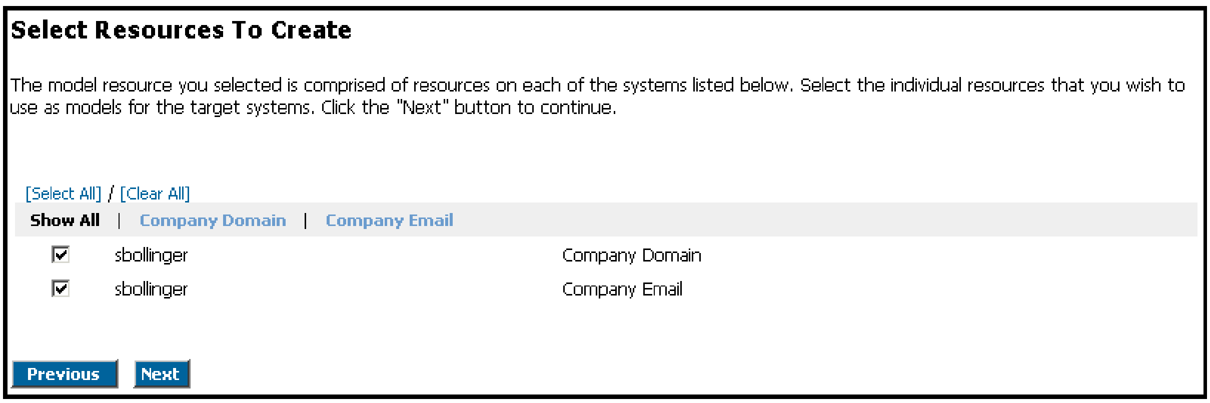
1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **CREATE**.
4. Click the icon next to **IDENTITYMAP SCREEN**.

The process to modify the fields for the IdentityMap Screen in the Create action of the Super-User workflow is the same as for a Create action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

In the Select Resources to Create screen, the names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. The targets that are displayed are determined by the accounts owned by the user selected as the baseline. (The targets must also be configured on the Target Configuration Form. For more details on configuring targets, refer to *Table 5 on page 245*.) For each target, the provisioner must select the baseline target by checking the checkbox if they want to create a new account for that target.

Figure 29: Select Resources to Create Screen



Configure an Initial Profile

In the CourionSuper-User sample workflow, the Initial Profile form is used to collect the account name of the end user. This information is then used to populate those fields in the Active Directory and Exchange accounts that are being created.

To modify the Initial Profile Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Initial Profile**.

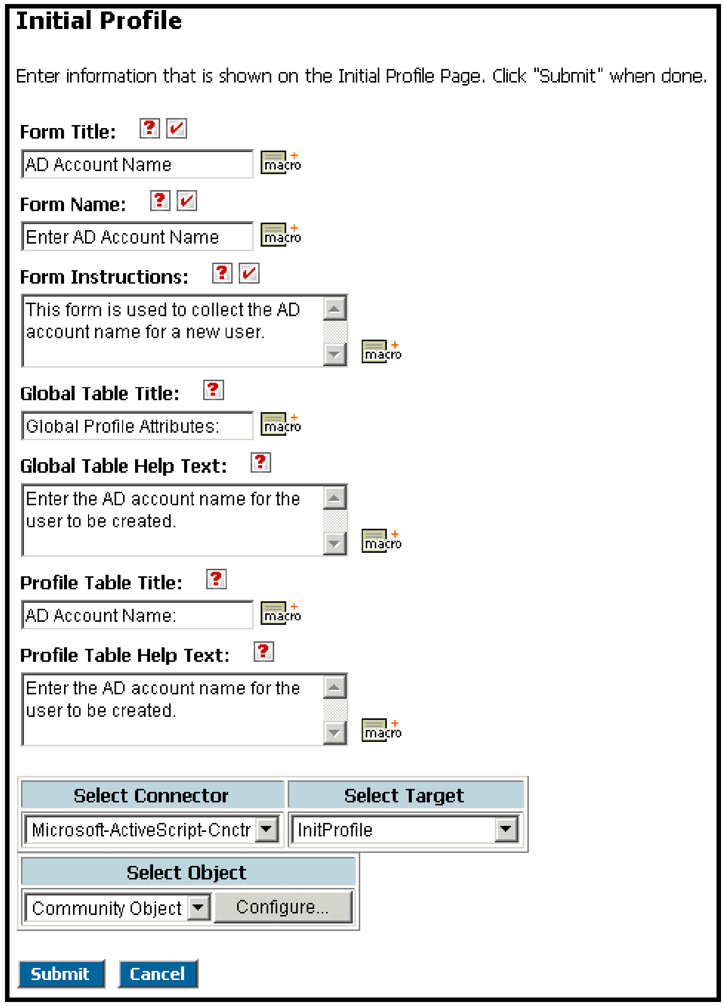
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Create**.

4. Click the icon next to **INITIAL PROFILE**.

   The Administration Manager displays the Initial Profile Form, shown in *Figure 30* with default text and sample data. All text boxes can be edited.

Figure 30: Initial Profile Form



5. Text in the **FORM TITLE** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **FORM NAME** text box appears as a title on the form.
7. Text in the **FORM INSTRUCTIONS** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. Text in the **GLOBAL TABLE TITLE** text box appears as the title on Global Fields Table.
9. Text in the **GLOBAL TABLE HELP TEXT** box appears as the help text in the Global Fields Table.
10. Text in the **PROFILE TABLE TITLE** text box appears as the title for each user’s profile table.
11. Text in the **PROFILE TABLE HELP TEXT** box appears as the help text in the Profile Table.

12. The **Select Connector**, **Select Target**, and **Select Object** fields are set to use a specific script for Microsoft Active Script, which passes the information collected here to the targets.

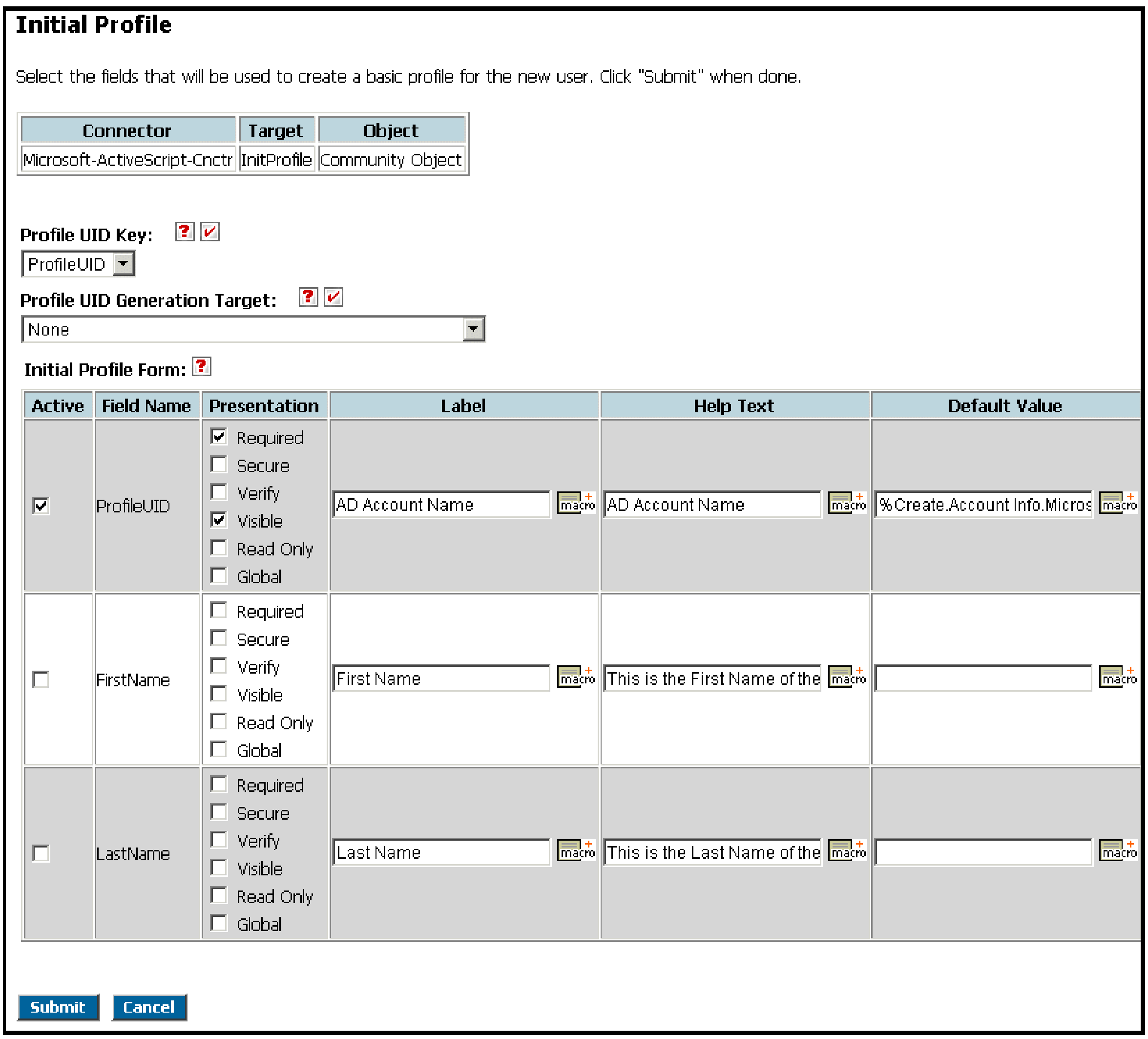
    Note: The Community Object script assigned in this workflow is designed to collect the account name. This field is needed for the creation of an Active Directory account. If you are adding other targets and need to collect additional information, you can edit the script to collect other information. Once collected, a macro is assigned on the Unique Target Data Field Selection Form to populate the appropriate attribute for the target.

13. Click **Configure...**.

    The Administration Manager displays the Initial Profile Select Fields Form, shown in *Figure 31*.

    Note: The fields displayed depend on the object selected.

Figure 31: Initial Profile Select Fields Form



14. Select the fields to include in the initial profile for a new user. Table 2 lists the columns shown in *Figure 31* and describes the required input.

    Table 3 describes the effects of the Initial Profile Field Selection Form options.

Table 2: Initial Profile Field Selection Form Options

Column Name	Input Description
Active[1]	Check to include the field in the initial profile record for a new user.
Field Name	Displays the field name.
Presentation	Includes the following options: • **Required**[1] — Check to ensure the field is included for all profiles created in this workflow. AccountCourier cannot create the initial profile if a required field value is null or invalid. Unchecked fields are optional. If a field value is not entered, AccountCourier creates the initial profile with a null value. • **Secure** — Check to display field input on the provisioner form as a series of asterisks (*****). It is good practice to mark a field as secure if that field has been marked hashed or encrypted in the Data Security Utility. It is good practice to require the provisioner to enter a value twice by selecting “Verify”. • **Verify** — Check to require double entry of the field value on the provisioner form. Fields with this option selected display two input boxes on the provisioner form, one with the label supplied in “Label” and second with the label “Verify”. • **Visible**[1] — Checked fields appear on the form displayed to the provisioner. By default, all fields are checked. Unchecked fields do not appear to the provisioner. This enables you to enter a value for the field that the provisioner cannot change. • **Read Only** — Check to display the field value to the provisioner without enabling the provisioner to edit the information. • **Global** — Check this box to specify that all profiles share the value in this field. Global fields appear in a Global Profile Attributes table at the top of the Initial Profile form. This option is useful with the bulk provisioning feature because you do not have to enter the same value for multiple profiles.
Label	Edit the default text or enter new text that names the field input box on the form displayed to the provisioner.
Help Text	Edit the default text or enter new text that appears when the provisioner moves the mouse pointer over the help icon for the field on the form.

Table 2: Initial Profile Field Selection Form Options

Column Name	Input Description
Default Value[1]	Enter a default value for the field.
Use for Acct Gen	Check to use the value as input for the AccountCourier automatic resource ID generation utility. For information on automatic name generation, see *Table 5 on page 245*.
Order	Enter a number for each selected field to determine the order the field names are listed. The field numbered “1” appears at the top of the list.

1. See Table 3 for an explanation of how these options work together.

Table 3: Selecting Fields and Default Values for an Initial Profile

Active	Required	Visible	Result
☑	☐	☐	Field selected. Field not required. Field not shown on provisioner form. You may enter a field value in the “Default Value” field. If you do not enter a value, AccountCourier creates the initial profile with a null value for the field.
☑	☑	☐	Field selected. Field required. Field not shown on provisioner form. You must enter a non-null value in the “Default Value” field.
☑	☑	☑	Field selected. Field required. Field shown on provisioner form. You may enter a field value in the “Default Value” field but the provisioner can override it. Null values are invalid.

Table 3: Selecting Fields and Default Values for an Initial Profile

Active	Required	Visible	Result
☑	☐	☑	Field selected. Field not required. Field shown on provisioner form. You may enter a field value in the “Default Value” field but the provisioner can override it. If neither the administrator or the provisioner enters a value, AccountCourier creates the initial profile with a null value for the field.
☐			Field not selected; is not included in initial profile

If you enter a default value for the field selected as the foreign key, mark the field **ACTIVE** and **REQUIRED**, and clear the **VISIBLE** column.

If the provisioner supplies the value, mark the field **ACTIVE**, **REQUIRED**, and **VISIBLE**.

15. The **PROFILE UID KEY** drop-down box lists all configured targets for resource creation.
16. The **PROFILE UID GENERATION TARGET** drop-down box lists the targets whose generated resource names may be used as the Profile UID key.
17. Click **SUBMIT**.

Figure 32 shows an example of the Initial Profile form that the provisioner sees.

Figure 32: Enter AD Account Name Screen

Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are used to provision accounts. The Unique Target Data form displays the currently available targets for which accounts can be created. The CourionSuper-User sample workflow has three targets already configured—the Transaction repository (for creation of an entry in the IdentityMap), Active Directory (for a logon ID) and Microsoft Exchange (for an email account). If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. Refer to *Table 5 on page 245* for information on this form.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, etc.

To modify the Unique Target Data Form:

Flowchart View

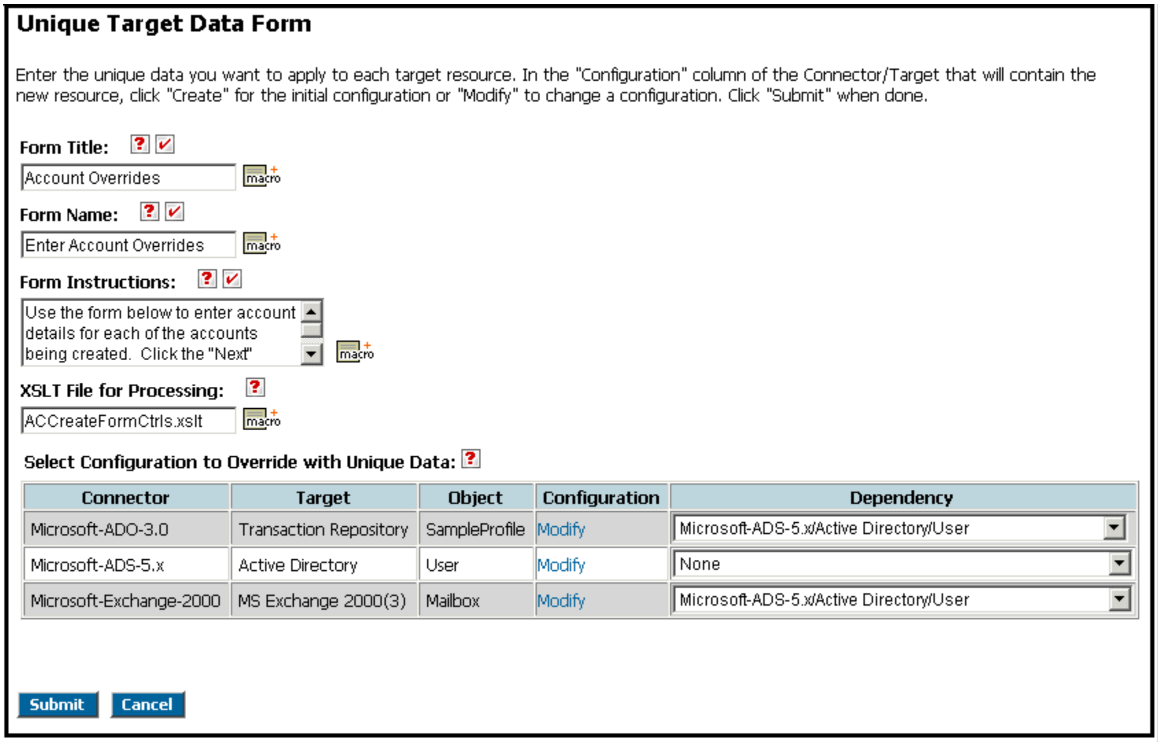
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the icon next to **Unique Resource Data.**

   The Administration Manager displays the Unique Target Data Form, shown in *Figure 33* with default text and sample data. All text boxes can be edited. Data fields depend on the available connectors and targets.

Figure 33: Unique Target Data Form



5. Text in the **FORM TITLE** text box appears in the title bar of the Web Access Client browser window.

6. Text in the **FORM NAME** text box appears as a title on the form.

7. Text in the **FORM INSTRUCTIONS** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)

8. Specify the file name or a macro that selects the **XSLT FILE FOR PROCESSING**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTLML controls are rendered, controlling how provisioners interact with the data.

   To customize an XSLT file, copy the default file provided by Courion and rename it. Then edit the renamed file as needed and assign that file to this field.

9. In the **DEPENDENCY** column, select the name of the target where the first resource must be successfully provisioned before any other resources are provisioned.

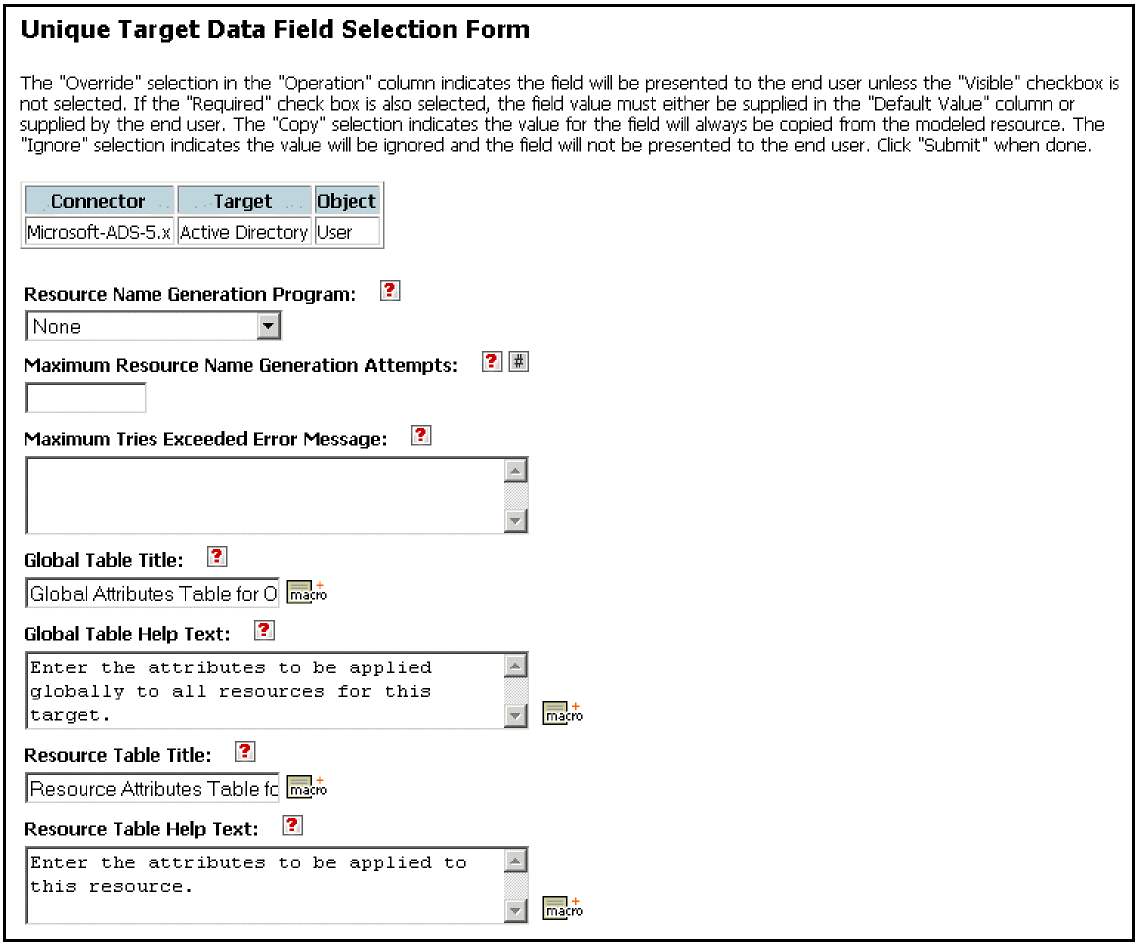
   Note: If you want Target C to be dependent on Target A and Target B, make the following dependency: Target C is dependent on Target B, which is dependent on Target A.

10. In the **CONFIGURATION** column, click **MODIFY** to change the attribute settings for the Transaction Repository, Active Directory, or Exchange accounts. If you have added any additional targets, click **CREATE**.

    The Administration Manager displays the Unique Target Data Field Selection Form (*Figure 34*).

    The actual content of this form depends on the connector. *Figure 34* shows the top of the form for the Connector for Microsoft Active Directory.

Figure 34: Unique Target Data Field Selection Form



Unique Target Data Field Selection Form

The "Override" selection in the "Operation" column indicates the field will be presented to the end user unless the "Visible" checkbox is not selected. If the "Required" check box is also selected, the field value must either be supplied in the "Default Value" column or supplied by the end user. The "Copy" selection indicates the value for the field will always be copied from the modeled resource. The "Ignore" selection indicates the value will be ignored and the field will not be presented to the end user. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADS-5.x	Active Directory	User

Resource Name Generation Program:

None

Maximum Resource Name Generation Attempts:

Maximum Tries Exceeded Error Message:

Global Table Title:

Global Attributes Table for O

Global Table Help Text:

Enter the attributes to be applied globally to all resources for this target.

Resource Table Title:

Resource Attributes Table fc

Resource Table Help Text:

Enter the attributes to be applied to this resource.

11. AccountCourier can automatically generate a resource name on each selected target system. In the CourionSuper-User workflow, the account name is entered in the Enter AD Account name screen, so this is option is not needed. But if you are configuring additional targets, this option can be used. For more info, see *Table 5 on page 245*.
12. Text in the **Global Table Title** text box appears as the heading for the Global Attributes table.
13. Text in the **Global Table Help Text** text box appears as the help for the Global Attributes table.
14. Text in the **Resource Table Title** text box appears as the heading for each Resource Attributes table.
15. Text in the **Resource Table Help Text** text box appears as the help for the Resource Attributes table.
16. Configure the attributes for the target. You can determine whether or not an attribute is exposed to the provisioner, whether it is required, whether the values may be mined from the Mining Community, etc. Up to twenty-five attributes for the selected target are displayed in the table. To view additional attributes, click the "next page" icon at the bottom of the table. Table 4 lists a description for the

column names of the Resource Attributes to Override table that appears at the bottom of the Unique Target Data Field Selection Form shown in *Figure 34*, and describes the required input.

Table 4: Choose Resource Attributes to Override Options

Column Name	Input Description
Operation	Includes the following options (**Note:** these options are dependent on the action and the attribute. Only applicable options are displayed.) • **Copy** — Copy the attribute from the source account and display it to the end user. This selection disables the remaining columns in the table for this attribute. • **Override** — Ignore the value of this attribute in the source account. Display the attribute to the end user (provided the **Visible** checkbox is selected). The information provided in the remaining columns in the table for this attribute determine how it is managed by the workflow. • **Ignore** — Ignore the value of this attribute in the source account and do not display it to the end user. This selection disables the remaining columns in the table for this attribute. No value is sent to the target system from the workflow. Instead, the target system determines the default value, if any.
Resource Attribute	Displays the field name.
Presentation	Includes the following options: • **Required** — A field with a grayed-out check mark for this option is required by the connector, requires a non-null value, and cannot be unchecked. If you mark a field "Required", input is required but not checked by the connector. Fields with the "Required" option unchecked do not require administrator or provisioner input. If a field value is not entered, AccountCourier creates the resource with a null value. • **Secure** — Check to display field input on the provisioner form as a series of asterisks (*****). It is good practice to mark a field as secure if that field has been marked hashed or encrypted in the Data Security Utility. It is good practice to require the provisioner to enter a value twice by selecting "Verify". **Note**: If you mark a field as both "Secure" and "Visible", the value of this attribute (from the source account) is not displayed to the end user. Instead, [Not Available] is displayed. • **Verify** — Check to require double entry of the field value on the provisioner form. Fields with this option selected display two input boxes on the provisioner form, one with the label supplied in "Label" and second with the label "Verify". • **Visible** — Uncheck to prevent the field from appearing on the form displayed to the provisioner. This enables you to enter a value for the field that the provisioner cannot change. By default, all fields are checked. **Note**: If a field is marked as "Required" but the "Visible" field is unchecked, then the attribute is treated as if it is NOT required.

Table 4: Choose Resource Attributes to Override Options

Column Name	Input Description
Presentation (continued)	• **Read Only** — Check this box to display the field to the provisioner but prevent the provisioner from modifying the data in the field. • **Global** — Check this box to specify that the value for this field is the same for all resources on this target. This option is useful with the bulk provisioning feature because you do not have to enter the same value for multiple resources. **Note**: If you select the "Global" option, the **Obtain Value From Source** and **Obtain Value From Provisionee** options have no effect. • **Mining** — Check this box to allow attribute values to be mined from the Mining Community. When this option is selected, a mining icon is displayed next to the attribute value. If the provisioner clicks on the icon, the attribute values belonging to the members of the mining community are displayed along with a percentage value showing what percentage of the mining community has that particular value. **Note**: To use this option, you must configure the Mining Community for use in the workflow and the end user must select one or more users to mine for attribute values. **Note:** If an attribute is marked as "Secure", "Read Only", or "Global", mining can not be used and this box should not be checked. The mining icon does not appear to the provisioner in this case, even if the box has been checked. **Note:** Not all attributes exposed on the unique resource data screen are actual attributes of the resource on the target system. Some are present on the unique resource data to provide information to the Connector on how to complete the specific action for that resource. For those attributes, mining is not possible, as there is no actual attribute whose value can be retrieved and hence mined. Many of these types of attributes return "n/a" in the current value or source value column.
Label	Edit the default text or enter new text that names the field input box on the provisioner form.
Help Text	Edit the default text or enter new text that appears when the provisioner moves the mouse pointer over the help icon for the field on the provisioner form. Some fields supply default help text.
Obtain Value From	Includes the following options (**Note:** these options are dependent on the attribute. Only applicable options are displayed.): • **Source** — Default value is set to the source resource's value for this attribute. • **Provisionee** — Default value is set to the provisionee resource's value for this attribute. • **Default Value** — Default value displayed is the value set as the default value of the control type in the attribute display options.

Table 4: Choose Resource Attributes to Override Options

Column Name	Input Description
Attribute Display Options	**Control type** determines the type and format of information that the user enters for the attribute. If you specified Default Value in the Obtain Value From column, you can enter a default value in the attribute display column or choose to leave it blank. If you supply a default value, it is displayed to the end user when they run the workflow. Options and the type of default value are listed below: • Basic List — ASCII text • Boolean — Check box • Conditional Boolean — Drop-down List • Custom List — ASCII text. In addition to the default value, a list of values is presented. • Date — Date values are in the form MM/DD/YYYY • E-mail — ASCII text in the form of a valid email address • Integer • List — Drop-down List • Membership — If you are configuring a Group Membership Attribute, click on the Configure link to access the Multi-Value Attribute form, and refer to *Table 5 on page 245* for details on this form. • Real Number — Can include a decimal point • Text — A single line of ASCII text • Text Area — Multiple lines of ASCII text • Time — Time values are in the form HH:MM:SS Enter a default value for this field if required. Some required fields have default values supplied by the connector.
Order	The Order column indicates the order in which the Unique Resource attribute appears to the end user on the Unique Target Data Screen.
Validation	If you have configured functions for this workflow, you can select the function here. Only configured functions appear as options in the Validation drop-down list, otherwise [N/A] appears.
Connector Datatype	This column displays the internal data type that the connector communicates to the Administration Manager. This provides a reference to the administrator when selecting the attribute display option. When selecting the control type for the attribute display option, you ensure that it is relevant to the connector data type. For example, if the connector data type was BOOL (Boolean), selecting a control type of Membership would create errors when running the workflow.

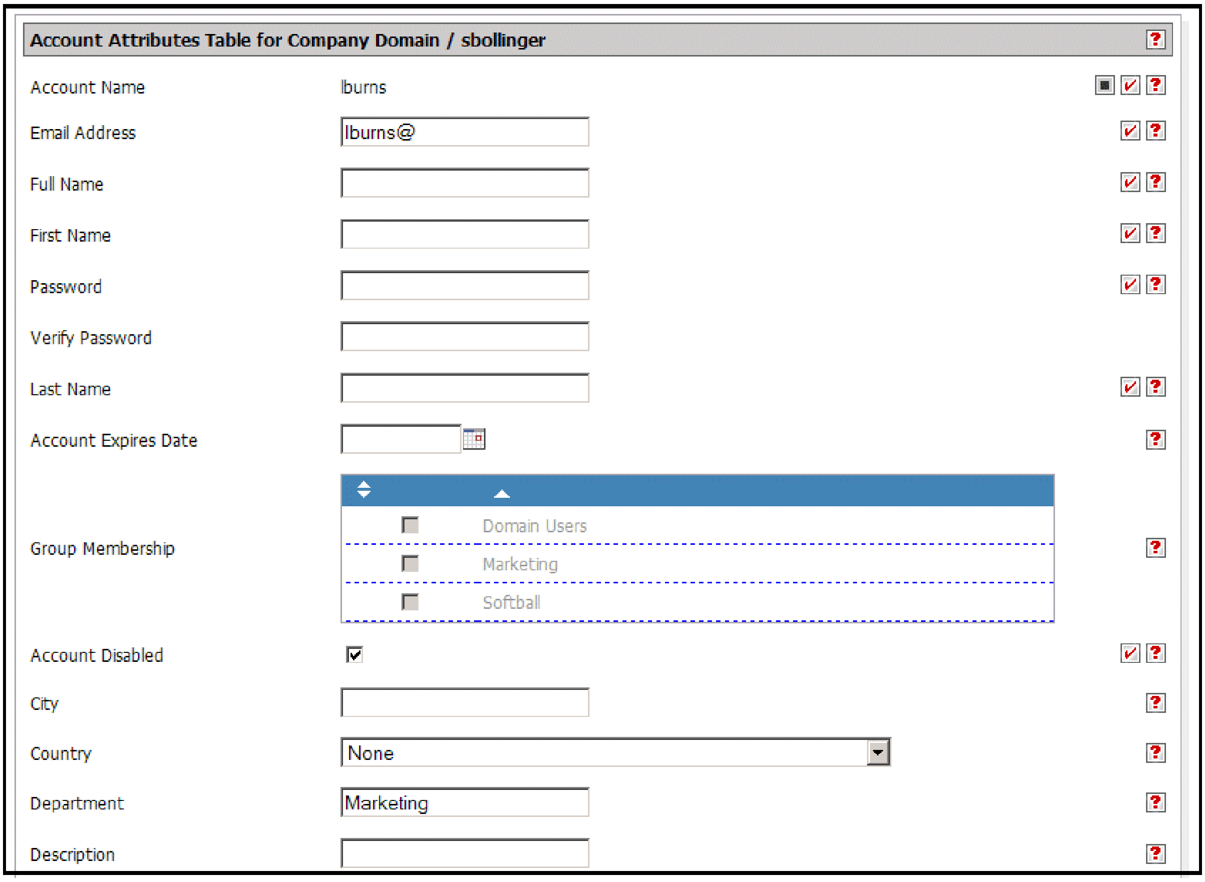
17. Click **SUBMIT** after completing the Unique Target Data Field Selection Form.

    The Administration Manager redisplays the Unique Target Data Form (*Figure 33*).

18. Click **CREATE** or **MODIFY** for another connector to configure the set of attributes for another resource or click **SUBMIT** to finish.

Figure 35 shows an example of part of the Enter Account Attributes screen displayed to the provisioner.

Figure 35: Enter Account Overrides Screen



Adding Accounts for an Existing User

This section describes how to configure the Add action, using the CourionSuper-User sample workflow.

With this workflow, a provisioner adds one or more accounts for an existing user. The Super-User workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing user for whom accounts need to be added.
3. Select a different user to serve as the baseline for the accounts being added.
4. Select the accounts to add.
5. Select individual attributes for each account being added. Default values for various attributes, based on the model account.

The following sections describe configuration of the forms needed for the Add action:

- *"Configure Properties for the Add Action" on page 81* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 84* describes how to set up a form the provisioner can complete to filter the profiles available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 85* describes how to set up a form that displays the available profiles. The provisioner selects the profile for which they want to add accounts.
- *"Refine the List of Displayed Resource Profiles" on page 89* describes how to set up a form the provisioner can complete to filter the profiles available in the workflow's resource community.
- *"Define a Resource Community" on page 90* describes how to set up a form that displays the user profiles available for modeling. The provisioner selects a profile and the provisioning application uses the unique identifier in the profile to search the IdentityMap for all the resources associated with the profile.
- *"Define the IdentityMap Screen Presentation for the Add Action" on page 91* describes how to set up a form that controls the appearance of the Select Accounts to Add form presented to the provisioner.
- *"Specify Unique Resource Data Fields for the Target" on page 92* describes how to set up a form the provisioner completes that specifies the fields, and possible default values, required to add the new resource.

The following instructions describe how to modify the settings in the CourionSuper-User workflow. If you have created a new workflow by copying CourionSuper-User, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the Add Action

To modify the Properties for Add Action Form:

Flowchart View

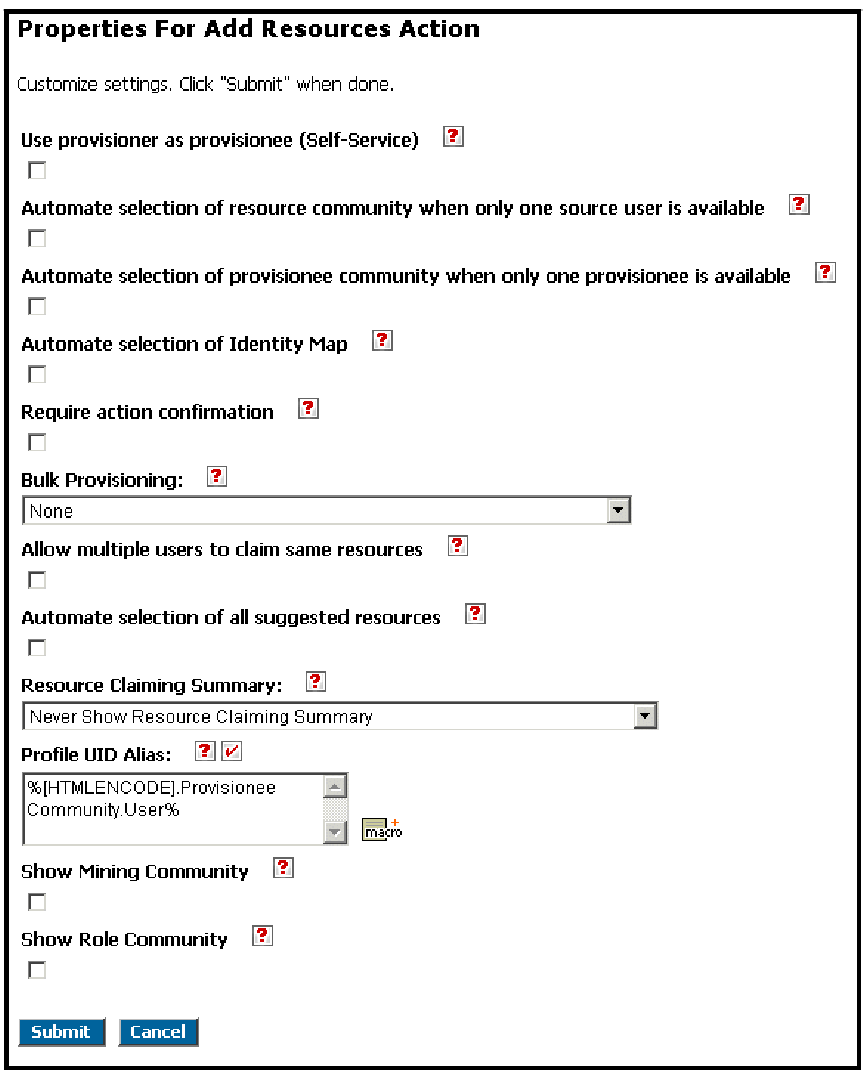
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Properties**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Properties**.

   The Administration Manager displays the Properties for Add Action Form, shown in *Figure 24*.

Figure 36: Properties for Add Action Form



5. Leave the **USE PROVISIONER AS PROVISIONEE (SELF-SERVICE)** checkbox unchecked, since it does not apply in this workflow.
6. Select the **AUTOMATE SELECTION OF RESOURCE COMMUNITY WHEN ONLY ONE SOURCE USER IS AVAILABLE** checkbox to enable automatic selection of the source profile (and bypass the Resource Community screen) when only a single source profile is retrieved from the connector. This setting is not selected by default.

   If you have created a special account as a baseline, check this checkbox. If you want the provisioner to be able to choose the baseline from a group of user accounts, leave the checkbox unchecked.
7. Select the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox to enable automatic selection of the provisionee profile (and to bypass the Provisionee Community screen) when only a single provisionee profile is retrieved from the connector. This setting is not selected by default.

   In the Super-User workflow, the provisionee is the user for whom you want to add accounts. Therefore, if this field is selected it would be necessary to authenticate into the workflow with the user's account name and password. So it is likely you will not want to select this field.
8. Select the **AUTOMATE SELECTION OF IDENTITYMAP** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **SUBMIT** button. This setting is turned off by default.

   In this workflow, the Resource Community is used to select a user as the baseline. Therefore, if this checkbox is selected, all of the baseline user's accounts are selected and created on all those targets. If an account already exists on a target, a second one is created. For this reason, you probably want to leave this box unchecked for an Add action.
9. Select the **REQUIRE ACTION CONFIRMATION** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.
10. Leave the **BULK PROVISIONING** option set to the default of None. This workflow does not use Bulk Provisioning.
11. Leave the **ALLOW MULTIPLE USERS TO CLAIM SAME RESOURCES** and **AUTOMATE SELECTION OF ALL SUGGESTED RESOURCES** checkboxes unchecked since this workflow does not use resource claiming.
12. Leave the **RESOURCE CLAIMING SUMMARY** option set to "Never show resource claiming summary" since this workflow does not use resource claiming.
13. The **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the CourionSuper-User sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
14. Leave the **SHOW MINING COMMUNITY** checkbox unselected since this workflow does not use the mining community.
15. Leave the **SHOW ROLE COMMUNITY** checkbox unselected since this workflow does not use the role community.
16. Click **SUBMIT**.

Refine the List of Displayed Provisionee Profiles

In the Add action of the Super-User workflow, the provisionee is the user for whom you want to add accounts.

By default, AccountCourier displays all the user account records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of accounts can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Provisionee Search screen (*Figure 37*). The provisioner enters values for one or more fields and AccountCourier searches the community and returns a list of accounts that meet the Provisionee Refine Search criteria. The provisioner then selects an account from the list for which accounts are added.

The provisioner can choose to skip entering data on the Provisionee Search screen. If the screen is skipped, AccountCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Provisionee Search screen is not displayed to the provisioner, by unchecking the **ACTIVE** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **ADD** from the navigation bar.
4. Click on **ADD REQUEST** and click on **PROVISIONEE REFINE SEARCH**.

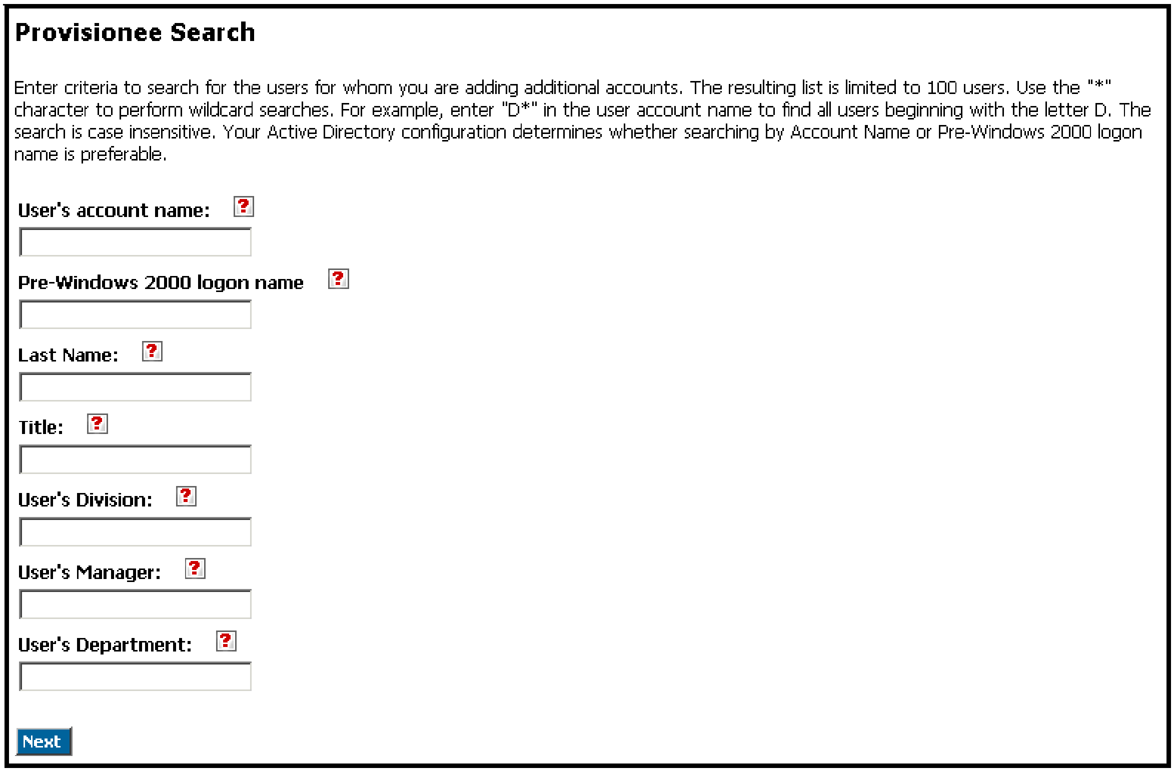
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **ADD**.
4. Click the icon next to **PROVISIONEE REFINE SEARCH**.

The process to refine the list of displayed profiles from a Provisionee Community in the Add action of the Super-User workflow is the same as for an Add action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

Figure 37 shows the screen displayed to provisioner, based on the settings from the Super-User workflow.

Figure 37: Provisionee Search



Define a Provisionee Community

In the Super-User workflow, the provisionee is the user for whom you want to add accounts. The Provisionee Community consists of user records in Active Directory.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **ADD** from the **ACTION** drop-down menu.
4. Click on **ADD REQUEST**.
5. Click on **PROVISIONEE COMMUNITY**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

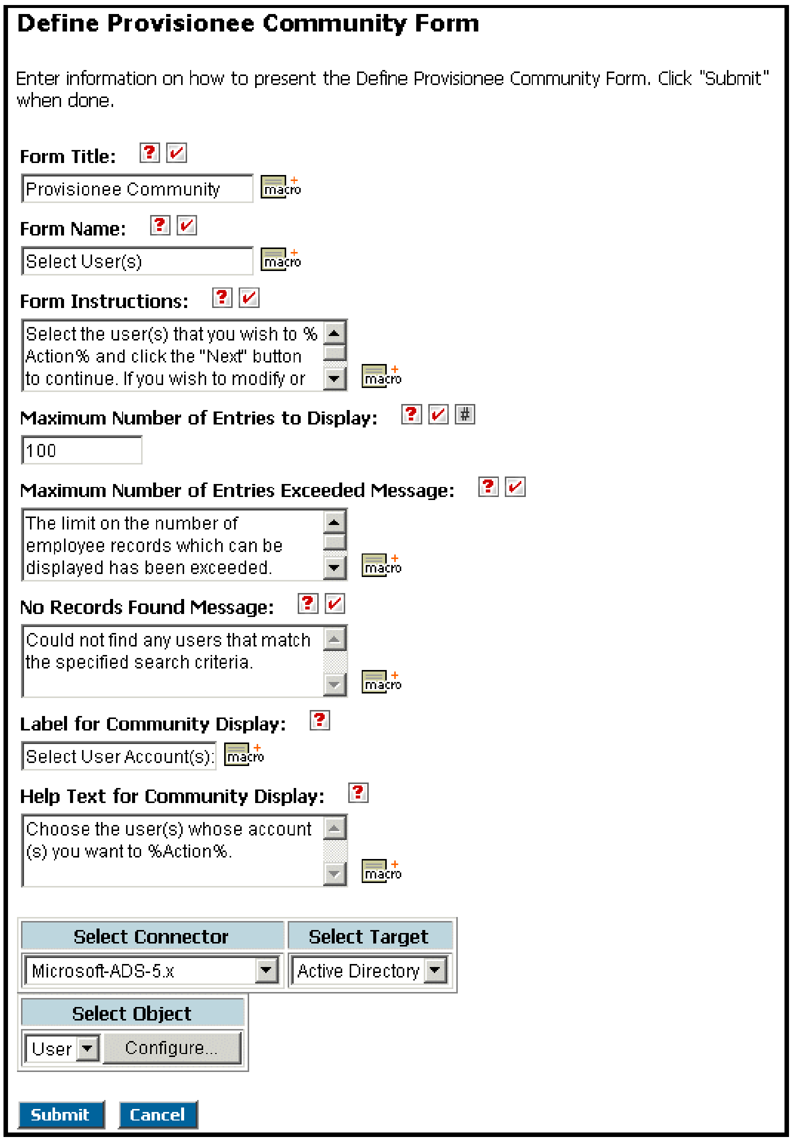
1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Click on **DYNAMIC COMMUNITIES** from the navigation bar.
4. Click on **PROVISIONEE COMMUNITY**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **GLOBAL SETTINGS**.
4. Click the icon next to **PROVISIONEE COMMUNITY**.

   The Administration Manager displays the Define Provisionee Community Form, shown in *Figure 38* with default text and sample data. You can edit all text boxes.

Figure 38: Define Provisionee Community Form



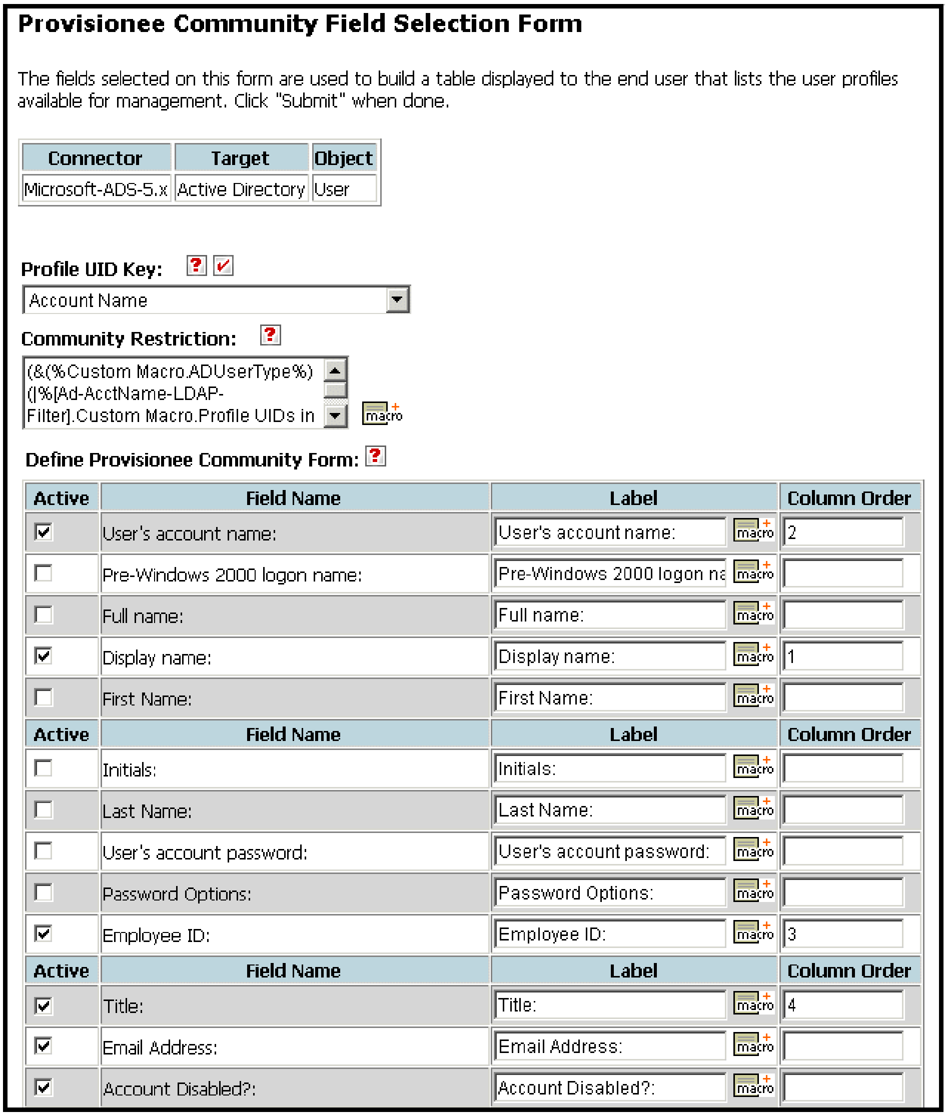
5. Text in the **FORM TITLE** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **FORM NAME** text box appears as a title on the form.
7. Text in the **FORM INSTRUCTIONS** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)

8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Provisionee Refine Search Form, can help the provisioner limit the number of returned profiles (see *"Refine the List of Displayed Provisionee Profiles" on page 84*).
9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Provisionee Refine Search Form to display profiles that more closely match search criteria.
10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message displays if the provisioner has entered values on the Provisionee Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Provisionee Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label for Community Display** text box appears as a title over the Mining Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Leave the **Select Connector** drop-down list box set to Microsoft-ADS-5.x, the **Select Target** drop-down list box set to Active Directory, and the **Object** drop-down list box set to User.
14. Click **Configure...**.

    The Administration Manager displays the Define Provisionee Community Field Selection Form, shown in *Figure 39*.

    Note: The list of fields has been shortened to save space.

Figure 39: Define Provisionee Community Field Selection Form



15. In the **PROFILE UID KEY** drop-down box, select the unique user ID field in this object that serves as a link to a user's entries, identified by the Profile UID field, in the Resource Community table.

16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Statement syntax depends on the target datasource. Do not use hashed or encrypted fields in the statement.

    In the Super-User workflow, the macro restricts return of available profiles to Active Directory records that belong to users, and only those users with a profile stored in the IdentityMap.

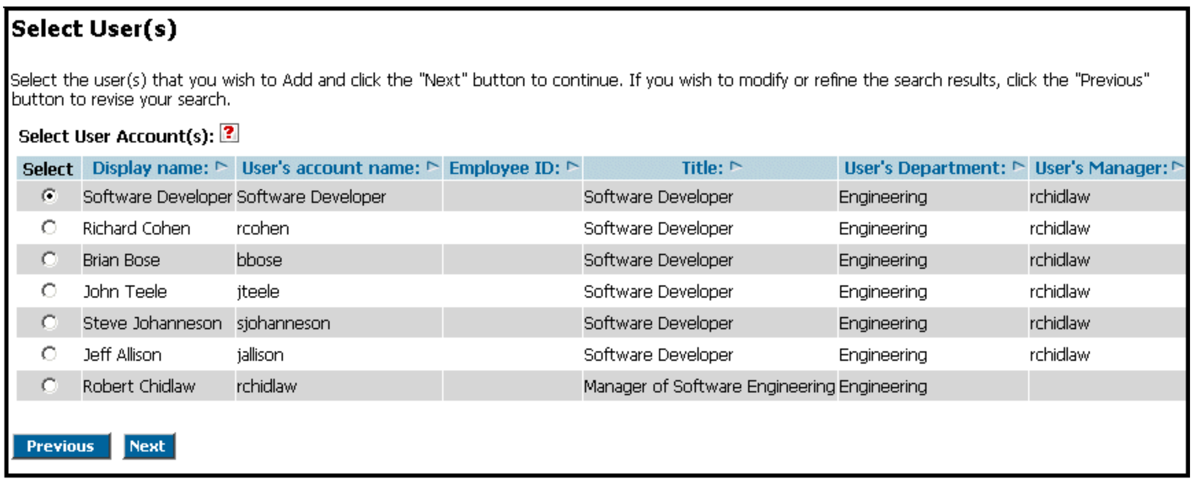
    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on Defining a Dynamic Community.

17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner.

18. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change an “EmployeeBadgeNumber” field to “Badge number:”.
19. In the **COLUMN ORDER** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered “1” appears as the first column.
20. Click **SUBMIT**.

Figure 40 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 40: Select User Screen



Select User(s)

Select the user(s) that you wish to Add and click the "Next" button to continue. If you wish to modify or refine the search results, click the "Previous" button to revise your search.

Select User Account(s):

Select	Display name:	User's account name:	Employee ID:	Title:	User's Department:	User's Manager:
◉	Software Developer	Software Developer		Software Developer	Engineering	rchidlaw
○	Richard Cohen	rcohen		Software Developer	Engineering	rchidlaw
○	Brian Bose	bbose		Software Developer	Engineering	rchidlaw
○	John Teele	jteele		Software Developer	Engineering	rchidlaw
○	Steve Johanneson	sjohanneson		Software Developer	Engineering	rchidlaw
○	Jeff Allison	jallison		Software Developer	Engineering	rchidlaw
○	Robert Chidlaw	rchidlaw		Manager of Software Engineering	Engineering	

Previous Next

Refine the List of Displayed Resource Profiles

The CourionSuper-User sample workflow uses the Resource Community to select a baseline user account as a model for adding accounts.

By default, AccountCourier displays all the users to the provisioner that meet the criteria configured in the Define Resource Community Form. If the filtering criteria for the Define Resource Community Form are broad or the company is large, the community of users could be extensive. You can select one or more fields to include on a Resource Refine Search Form. These fields are presented to the provisioner. The provisioner enters values for one or more fields and AccountCourier searches the community and returns a list of users that meet the Resource Refine Search criteria. The provisioner then selects a user from the list as a model.

The provisioner can choose to skip entering data on this form. If the form is skipped, AccountCourier returns all the user profiles established by the Define Resource Community Form. See *“Define a Resource Community” on page 90*.

To modify the Resource Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **ADD** from the **ACTION** drop-down menu.

4. Click on **Add Request**.
5. Click on **Resource Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Resource Refine Search**.

The process to modify the Resource Refine Search in the Add Action of the Super-User workflow is the same as for a Create Action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Define a Resource Community

The Add action in the CourionSuper-User sample workflow uses the Resource Community to select a baseline user account as a model for selecting accounts to be added to the provisionee. It is important to choose a baseline user account that has the target accounts that you want to add, or you cannot add those targets.

By using the Community Restriction parameter, found on the Resource Community Field Selection Form, you can restrict the resources that the provisioner can access. For example, you can set up a list that includes only the members of the Engineering department and restrict the provisioner to only provisioning resources associated with those members of the Engineering Department.

In practice, the Community Restriction parameter is often used to select a single baseline user. This ensures that all necessary targets are available for the provisionee. In this case, you can select the **Automate selection of resource community when only one source user is available** checkbox on the Properties Form, to enable automatic selection of the source profile (and bypass both the Resource Community and resource Refine Search screens).

Note: The Resource Community is global and affects all actions within a workflow. Therefore, any changes made apply to all actions in the Super-User workflow.

To modify the Define Resource Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Resource Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.

3. Click on **DYNAMIC COMMUNITIES** from the navigation bar.
4. Click on **RESOURCE COMMUNITY**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **GLOBAL SETTINGS**.
4. Click the icon next to **RESOURCE COMMUNITY**.

The process to configure the Resource Community for an Add Action is the same as for a Create Action.

To complete the Resource Community Form and the forms that follow, complete the steps described in *"Define a Resource Community" on page 63*.

Define the IdentityMap Screen Presentation for the Add Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Add Screen, shown in *Figure 41*.

Note: If the **AUTOMATE SELECTION OF IDENTITYMAP** on the Properties form is enabled, this form is skipped in the workflow, all of the baseline user's accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter Account Overrides screen to the provisioner).

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **BUSINESS PROCESS** and **ADD** from the navigation bar.
3. Click on **ADD REQUEST** and click on **IDENTITYMAP SCREEN**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the workflow.
3. Expand **ACTIONS**, expand **ADD**, and expand **ACTION SETTINGS**.
4. Click the icon next to **IDENTITYMAP SCREEN**.

The process to modify the fields for the IdentityMap Screen in the Add action of the Super-User workflow is the same as for an Add action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

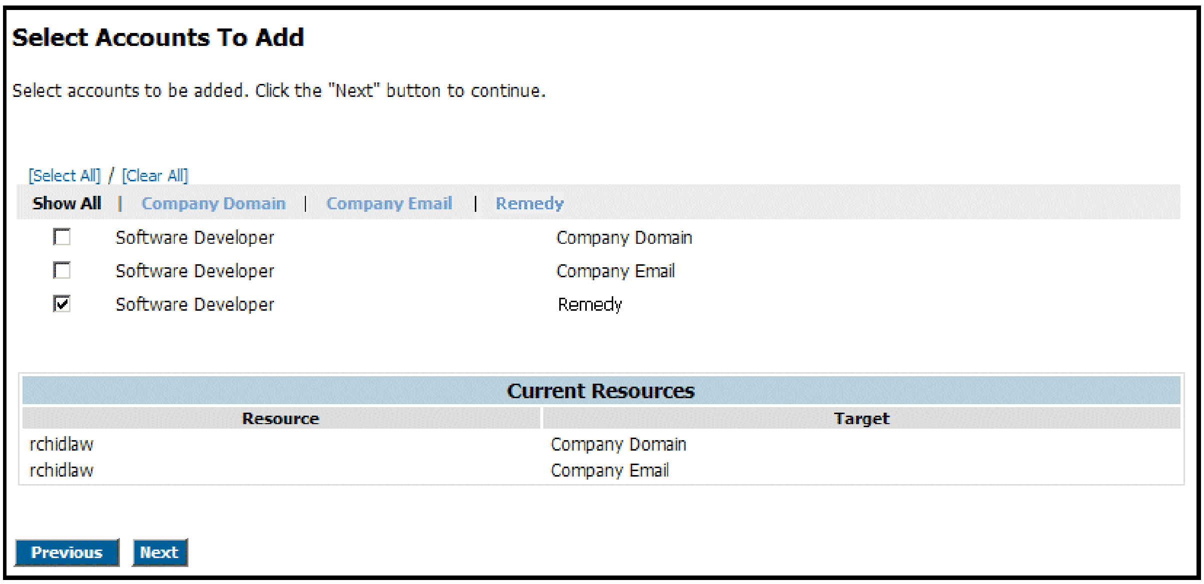
In the example *Figure 41*, a Remedy account is being added to the provisionee. The names of the individual targets in the grey menu bar are taken from the **ALIAS** field on the Add and Modify Target forms. If no alias is specified, the **IDENTITYMAP TARGET ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. The targets that are displayed are determined by the accounts owned by the user selected as the baseline. The targets must also be configured on the Target Configuration Form. (For more details on configuring targets, see *Table 5 on page 245*.)

Below the list of target accounts that belong to the model user is a list of current accounts belonging to the provisionee. This is provided as a reference, to help prevent creation of duplicate accounts on a specific target

For each target in which the provisioner wants to add an account, the provisioner must select the target by checking the checkbox.

Figure 41: Select Accounts to Add Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Resource Data form to configure which attributes are used to provision the accounts that are being added. The Unique Target Data form displays the currently available targets for which accounts can be created. The CourionSuper-User sample workflow has two targets already configured - Active Directory (for a logon ID) and Microsoft Exchange (for an email account). Before you can add other targets, they must first be configured on the Target Configuration form found in the global settings. For more details on configuring targets, see *Table 5 on page 245*.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which displays mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.

5. Click on **UNIQUE RESOURCE DATA**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **ADD**.
4. Click the  icon next to **UNIQUE RESOURCE DATA**.

The steps to complete the Unique Target Data Form to add a resource are the same as to create a resource. Follow the instructions provided in *"Specify Unique Resource Data Fields for the Target" on page 74*.

Change Attributes for an Existing Account

This section describes how to configure the Change action, using the CourionSuper-User sample workflow.

With this workflow, a provisioner selects accounts and changes the values of selected attributes for those accounts. The Super-User workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select a provisionee profile.
3. Select the provisionee's accounts that need to be changed.
4. Select individual attributes for each account and change the values as needed.

The following sections describe configuration of the forms needed for the Change action:

- *"Configure Properties for the Change Resources Action" on page 94* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 96* describes how to set up a form the provisioner can complete to filter the profiles available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 97* describes how to set up a form that displays the available profiles. The provisioner selects the profile for which they want to change account attributes.
- *"Define the IdentityMap Screen Presentation for the Change Action" on page 98* describes how to set up a form that controls the appearance of the Select Accounts to Change form presented to the provisioner.
- *"Specify Unique Resource Data Fields for the Target" on page 99* describes how to set up a form the provisioner uses to change attribute values.

The following instructions describe how to modify the settings in the CourionSuper-User workflow. If you have created a new workflow by copying CourionSuper-User, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the Change Resources Action

To modify the Properties for Change Resources Action Form:

Flowchart View

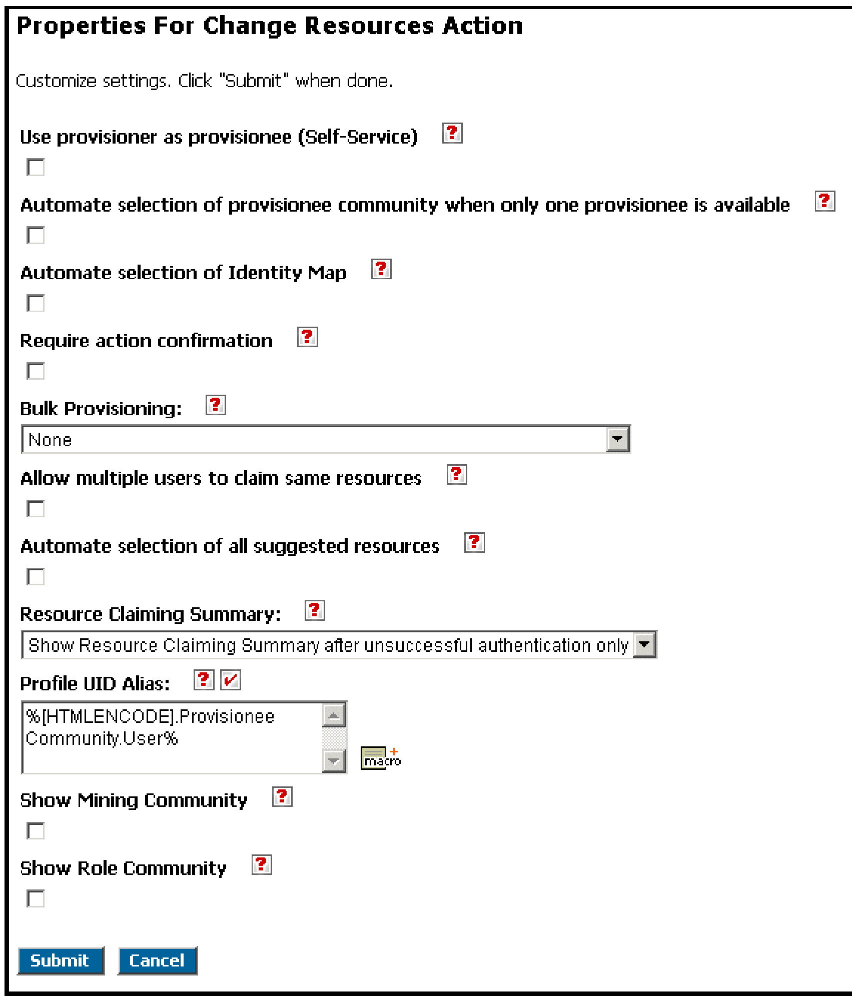
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the **Action** drop-down menu.
4. Click on **Change Request**.
5. Click on **Properties**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **CHANGE**.
4. Click the icon next to **PROPERTIES**.

   The Administration Manager displays the Properties for Change Resources Action Form, shown in *Figure 42*.

Figure 42: Properties for Change Resources Action Form



5. Leave the **USE PROVISIONER AS PROVISIONEE (SELF-SERVICE)** checkbox unchecked, since it does not apply in this workflow.
6. Select the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox to enable automatic selection of the provisionee profile (and to bypass the Provisionee Community screen) when only a single provisionee profile is retrieved from the connector. This setting is not selected by default.

   In the Super-User workflow, the provisionee is the user for whom you want to change account attributes. Therefore, if this field is selected it would be necessary to authenticate into the workflow with the user's account name and password. So it is likely you will not want to select this field.

7. Select the **AUTOMATE SELECTION OF IDENTITYMAP** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **SUBMIT** button. This setting is turned off by default.
8. Select the **REQUIRE ACTION CONFIRMATION** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.
9. Leave the **BULK PROVISIONING** option set to the default of None. This workflow does not use Bulk Provisioning.
10. Leave the **ALLOW MULTIPLE USERS TO CLAIM SAME RESOURCES** and **AUTOMATE SELECTION OF ALL SUGGESTED RESOURCES** checkboxes unchecked since this workflow does not use resource claiming.
11. Leave the **RESOURCE CLAIMING SUMMARY** option set to “Show Resource Claiming Summary after unsuccessful authentication only”.
12. The **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the CourionSuper-User sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
13. Leave the **SHOW MINING COMMUNITY** checkbox unselected since this workflow does not use the mining community.
14. Leave the **SHOW ROLE COMMUNITY** checkbox unselected since this workflow does not use the role community.
15. Click **SUBMIT**.

Refine the List of Displayed Provisionee Profiles

In the Change action of the Super-User workflow, the provisionee is the user for whom you want to change account attributes.

By default, AccountCourier displays all the user account records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of accounts can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Provisionee Search screen (*Figure 43*). The provisioner enters values for one or more fields and AccountCourier searches the community and returns a list of accounts that meet the Provisionee Refine Search criteria. The provisioner then selects an account from the list for which accounts are added.

The provisioner can choose to skip entering data on the Provisionee Search screen. If the screen is skipped, AccountCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Provisionee Search screen is not displayed to the provisioner, by unchecking the **ACTIVE** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.

3. Select **BUSINESS PROCESS** and **CHANGE** from the navigation bar.
4. Click on **CHANGE REQUEST** and click on **PROVISIONEE REFINE SEARCH**.

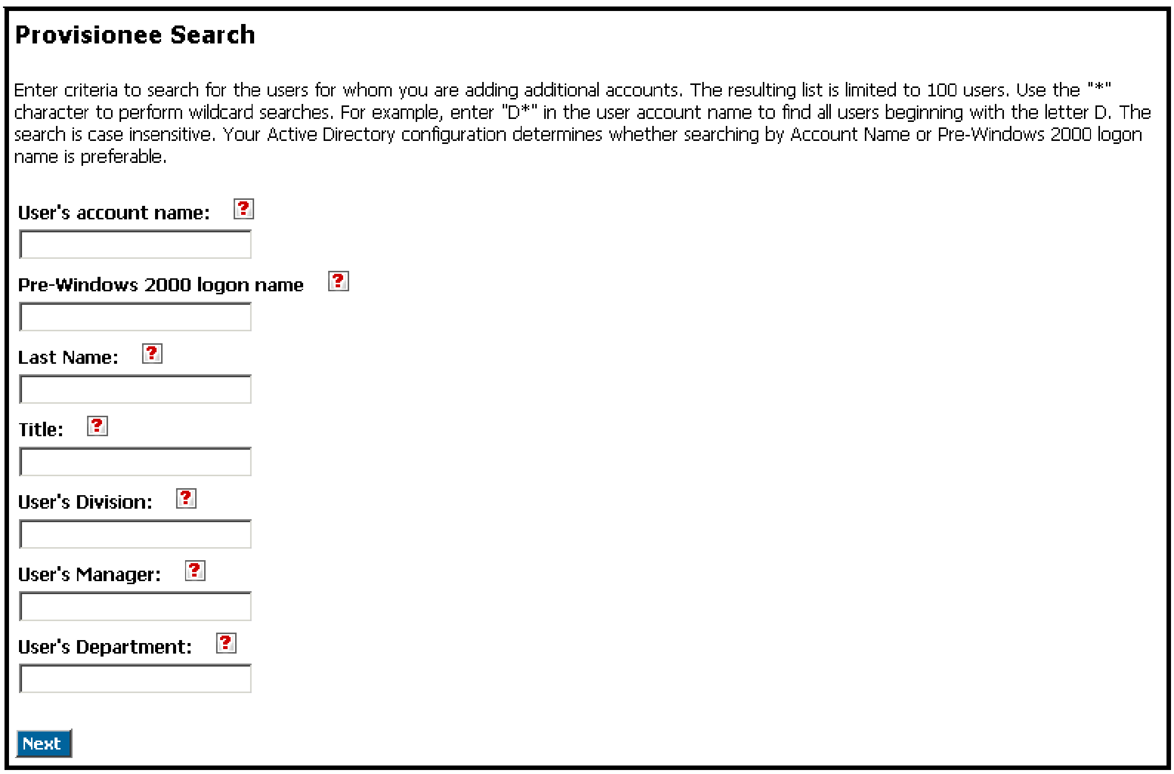
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **CHANGE**.
4. Click the icon next to **PROVISIONEE REFINE SEARCH**.

The process to refine the list of displayed profiles from a Provisionee Community in the Change action of the Super-User workflow is the same as in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

Figure 43 shows the screen displayed to provisioner, based on the settings from the Super-User workflow.

Figure 43: Provisionee Search Screen



Provisionee Search

Enter criteria to search for the users for whom you are adding additional accounts. The resulting list is limited to 100 users. Use the "*" character to perform wildcard searches. For example, enter "D*" in the user account name to find all users beginning with the letter D. The search is case insensitive. Your Active Directory configuration determines whether searching by Account Name or Pre-Windows 2000 logon name is preferable.

User's account name:

Pre-Windows 2000 logon name

Last Name:

Title:

User's Division:

User's Manager:

User's Department:

Next

Define a Provisionee Community

In the Change action of the Super-User workflow, the provisionee is the user for whom you want to add accounts. The Provisionee Community consists of the user records in Active Directory.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the **Action** drop-down menu.
4. Click on **Change Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

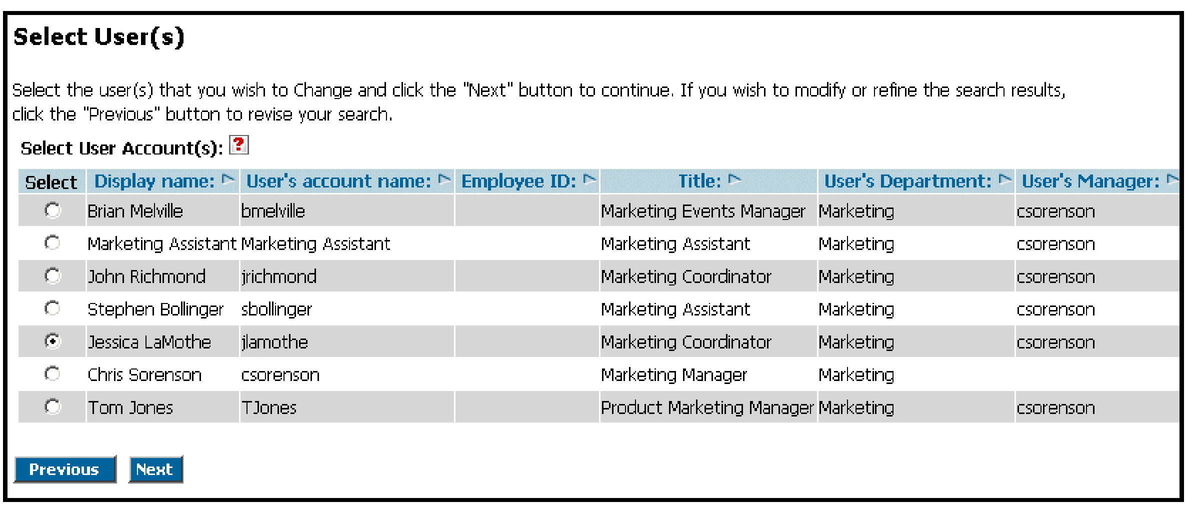
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Provisionee Community**.

   The process to define the Provisionee Community in the Change action of the Super-User workflow is the same as in the Add action. See *"Define a Provisionee Community" on page 85* for information about how to complete this form.

Figure 44 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 44: Select Users Screen


Select User(s)

Select the user(s) that you wish to Change and click the "Next" button to continue. If you wish to modify or refine the search results, click the "Previous" button to revise your search.

Select User Account(s):

Select	Display name:	User's account name:	Employee ID:	Title:	User's Department:	User's Manager:
○	Brian Melville	bmelville		Marketing Events Manager	Marketing	csorenson
○	Marketing Assistant	Marketing Assistant		Marketing Assistant	Marketing	csorenson
○	John Richmond	jrichmond		Marketing Coordinator	Marketing	csorenson
○	Stephen Bollinger	sbollinger		Marketing Assistant	Marketing	csorenson
◉	Jessica LaMothe	jlamothe		Marketing Coordinator	Marketing	csorenson
○	Chris Sorenson	csorenson		Marketing Manager	Marketing	
○	Tom Jones	TJones		Product Marketing Manager	Marketing	csorenson

Previous Next

Define the IdentityMap Screen Presentation for the Change Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Change screen, shown in *Figure 45*.

Note: If the **Automate selection of IdentityMap** on the Properties form is enabled, this form is skipped in the workflow, all of the provisionee's accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter Account Details screen to the provisioner).

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the navigation bar.
4. Click on **Change Request** and click on **IdentityMap Screen**.

Tree View

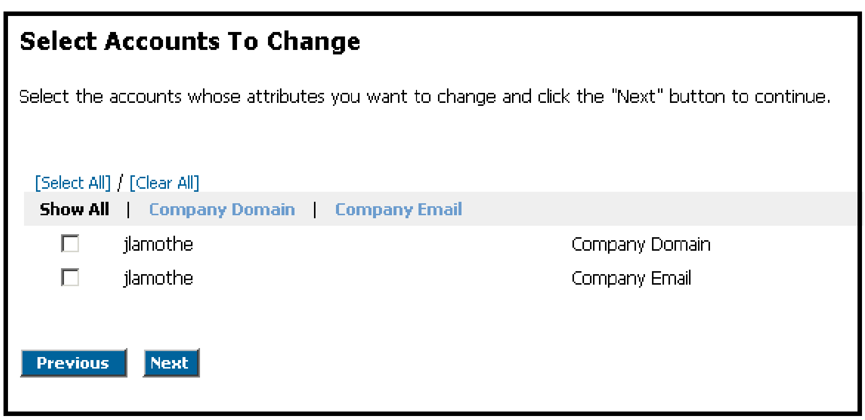
1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **Change**, expand **Action Settings**, and click the icon next to **IdentityMap Screen**.

The process to modify the fields for the IdentityMap Screen in the Change action of the Super-User workflow is the same as for a Change action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

The names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. For each target, the provisioner must select the target by checking the checkbox, if they want to change attributes for that target.

Figure 45: Select Accounts to Change Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are displayed to the provisioner. The CourionSuper-User sample workflow has two targets already configured - Active Directory (for a logon ID) and Microsoft Exchange (for an email account). If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. See *Table 5 on page 245* for details.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which displays mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the **Action** drop-down menu.
4. Click on **Change Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Change**.
4. Click the  icon next to **Unique Resource Data**.

The steps to complete the Unique Target Data Form to change a resource are the same as to create a resource. Follow the instructions provided in *"Specify Unique Resource Data Fields for the Target" on page 74*.

Disabling and Enabling Accounts

This section describes how to configure the Disable and Enable actions using the CourionSuper-User sample workflow. These actions enable a provisioner to disable and enable an account.

With this workflow, a provisioner selects a provisionee profile that is stored in the transaction repository, and then disables or enables the provisionee's accounts. Accounts may be disabled or enabled individually. The Super-User workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing provisionee.
3. Select the provisionee's accounts to disable or enable.

The steps to configure the forms for the Disable and Enable actions are virtually identical. Therefore, while the following descriptions of each form refers to the Disable action, they also apply to the Enable action.

The following sections describe configuration of the forms needed for the Disable and Enable actions:

- *"Configure Properties for the Disable Resources Action" on page 101* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 103* describes how to set up a form the provisioner can complete to filter the profiles available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 104* describes how to set up a form that displays the available profiles. The provisioner selects the provisionee for which they want to disable accounts.
- *"Define the IdentityMap Screen Presentation for the Disable Action" on page 105* describes how to set up a form that controls the appearance of the Select Accounts to Disable form presented to the provisioner.
- *"Specify Unique Resource Data Fields for the Target" on page 106* describes how to set up a form the provisioner completes that specifies the fields and possible default values, used when disabling an account.

The following instructions describe how to modify the settings in the CourionSuper-User workflow. If you have created a new workflow by copying CourionSuper-User, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the Disable Resources Action

To modify the Properties for Disable Resources Action Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **DISABLE** from the **ACTION** drop-down menu.

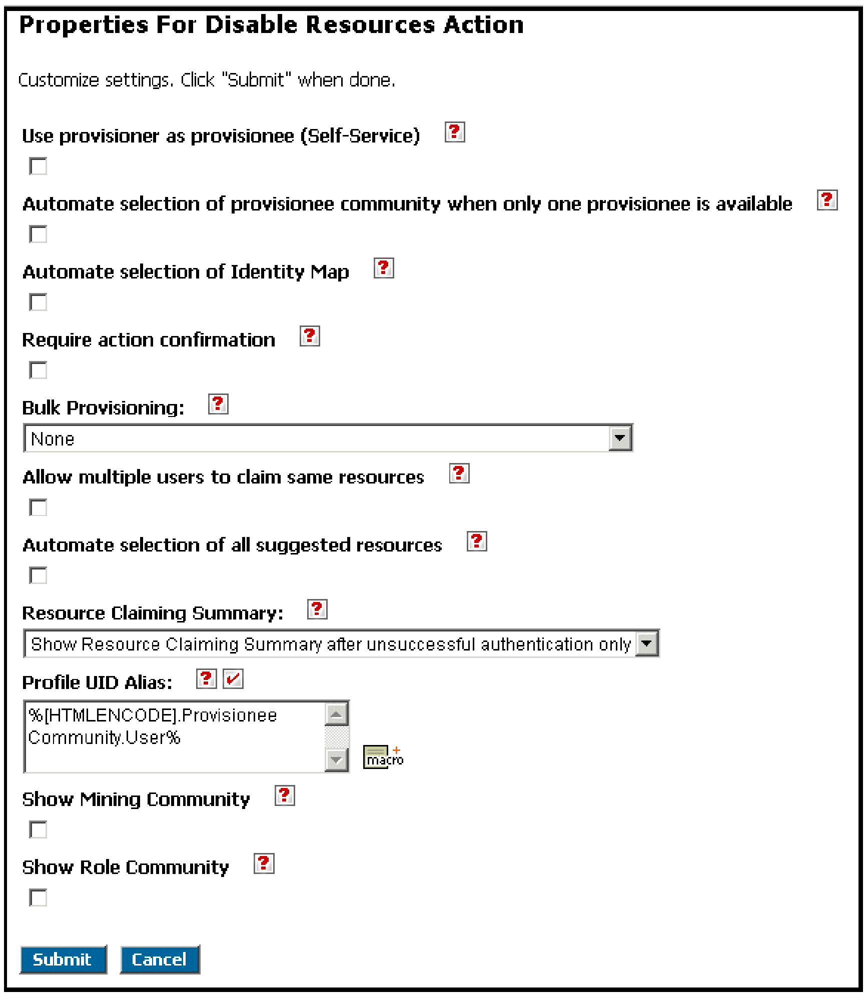
4. Click on **DISABLE REQUEST**.
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **DISABLE**.
4. Click the icon next to **PROPERTIES**.

   The Administration Manager displays the Properties for Disable Resources Action Form, shown in *Figure 46*.

Figure 46: Properties for Disable Resources Action Form



5. Leave the **USE PROVISIONER AS PROVISIONEE (SELF-SERVICE)** checkbox unchecked, since it does not apply in this workflow.
6. Select the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox to enable automatic selection of the provisionee profile (and to bypass the Provisionee Community screen) when only a single provisionee profile is retrieved from the connector. This setting is not selected by default.

In the Super-User workflow, the provisionee is the user for whom you want to change account attributes. Therefore, if this field is selected it would be necessary to authenticate into the workflow with the user's account name and password. So it is likely you will not want to select this field.

7. Select the **AUTOMATE SELECTION OF IDENTITYMAP** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **SUBMIT** button. This setting is turned off by default.
8. Select the **REQUIRE ACTION CONFIRMATION** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.
9. Leave the **BULK PROVISIONING** option set to the default of None. This workflow does not use Bulk Provisioning.
10. Leave the **ALLOW MULTIPLE USERS TO CLAIM SAME RESOURCES** and **AUTOMATE SELECTION OF ALL SUGGESTED RESOURCES** checkboxes unchecked since this workflow does not use resource claiming.
11. Leave the **RESOURCE CLAIMING SUMMARY** option set to "Show Resource Claiming Summary after unsuccessful authentication only".
12. The **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the CourionSuper-User sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
13. Leave the **SHOW MINING COMMUNITY** checkbox unselected since this workflow does not use the mining community.
14. Leave the **SHOW ROLE COMMUNITY** checkbox unselected since this workflow does not use the role community.
15. Click **SUBMIT**.

Refine the List of Displayed Provisionee Profiles

In the Disable action of the Super-User workflow, the provisionee is the user for whom you want to disable accounts.

By default, AccountCourier displays all the user account records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of accounts can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Provisionee Search screen (*Figure 43*). The provisioner enters values for one or more fields and AccountCourier searches the community and returns a list of accounts that meet the Provisionee Refine Search criteria. The provisioner then selects an account from the list for which accounts are added.

The provisioner can choose to skip entering data on the Provisionee Search screen. If the screen is skipped, AccountCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Provisionee Search screen is not displayed to the provisioner, by unchecking the **ACTIVE** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Disable** from the navigation bar.
4. Click on **Disable Request** and click on **Provisionee Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Disable**.
4. Click the icon next to **Provisionee Refine Search**.

The process to refine the list of displayed profiles from a Provisionee Community in the Disable action of the Super-User workflow is the same as in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

Define a Provisionee Community

In the Disable action of the Super-User workflow, the provisionee is the user for whom you want to disable accounts. The Provisionee Community consists of the account records in Active Directory.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Disable** from the **Action** drop-down menu.
4. Click on **Disable Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

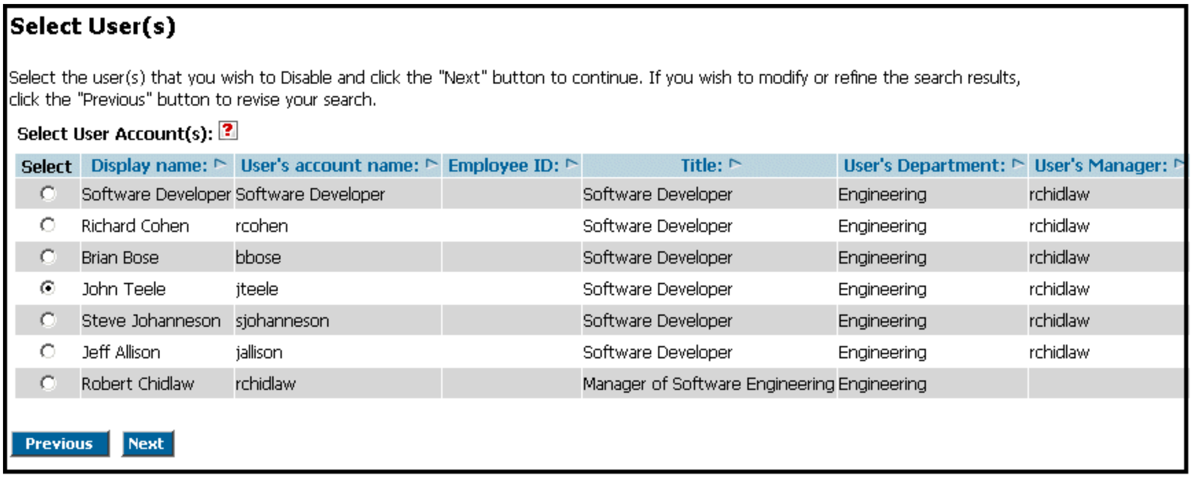
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Provisionee Community**.

The process to define the Provisionee Community in the Disable action of the Super-User workflow is the same as in the Add action. See *“Define a Provisionee Community” on page 85* for information about how to complete this form.

Figure 47 shows the screen displayed to provisioner.

Figure 47: Select Users Screen



Select User(s)

Select the user(s) that you wish to Disable and click the "Next" button to continue. If you wish to modify or refine the search results, click the "Previous" button to revise your search.

Select User Account(s):

Select	Display name:	User's account name:	Employee ID:	Title:	User's Department:	User's Manager:
○	Software Developer	Software Developer		Software Developer	Engineering	rchidlaw
○	Richard Cohen	rcohen		Software Developer	Engineering	rchidlaw
○	Brian Bose	bbose		Software Developer	Engineering	rchidlaw
◉	John Teele	jteele		Software Developer	Engineering	rchidlaw
○	Steve Johanneson	sjohanneson		Software Developer	Engineering	rchidlaw
○	Jeff Allison	jallison		Software Developer	Engineering	rchidlaw
○	Robert Chidlaw	rchidlaw		Manager of Software Engineering	Engineering	

Previous Next

Define the IdentityMap Screen Presentation for the Disable Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Disable screen, shown in *Figure 48*.

Note: If the **AUTOMATE SELECTION OF IDENTITYMAP** on the Properties form is enabled, this form is skipped in the workflow, all of the user’s accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter Comment screen to the provisioner).

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **DISABLE** from the navigation bar.
4. Click on **DISABLE REQUEST** and click on **IDENTITYMAP SCREEN**.

Tree View

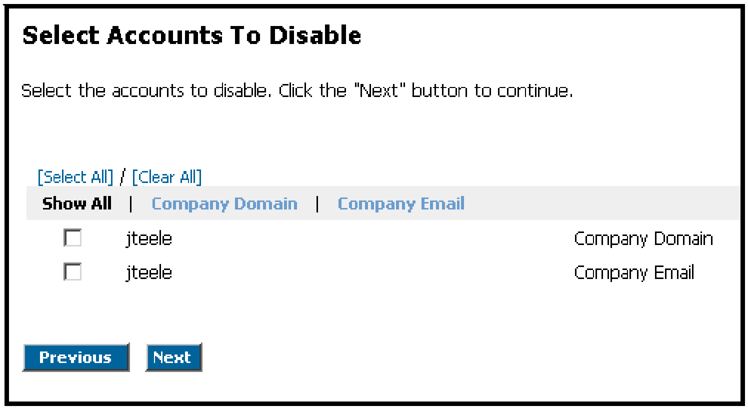
1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS**, expand **DISABLE**, expand **ACTION SETTINGS**, and click the icon next to **IDENTITYMAP SCREEN**.

The process to modify the fields for the IdentityMap Screen in the Disable action of the Super-User workflow is the same as for a Change action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

The names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. For each target, the provisioner must select the target by checking the checkbox, if they want to change attributes for that target.

Figure 48: Select Accounts to Disable Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are displayed to the provisioner. For the purpose of disabling or enabling an account, it is not necessary to expose any attributes. However, depending on the target and the available attributes, it can be useful to expose certain attributes. For example, some targets provide an attribute for comments, which can be used to document the reason for the disabling action.

If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. See *Table 5 on page 245* for details.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which displays mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Disable** from the **Action** drop-down menu.
4. Click on **Disable Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Disable**.

4. Click the icon next to **UNIQUE RESOURCE DATA**.

The steps to complete the Unique Target Data Form to Disable a resource are the same as to create a resource. Follow the instructions provided in *“Specify Unique Resource Data Fields for the Target” on page 74*.

Deleting Accounts

This section describes how to configure the Delete action using the CourionSuper-User sample workflow. This action enables a provisioner to delete individual provisionee accounts.

With this workflow, a provisioner selects a use, and then chooses which of the provisionee's accounts to delete. The Super-User workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing provisionee.
3. Select the provisionee's accounts to delete.

The following sections describe configuration of the forms needed for the Delete action:

- *"Configure Properties for the Delete Resources Action" on page 108* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 109* describes how to set up a form the provisioner can complete to filter the accounts available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 110* describes how to set up a form that displays the available profiles. The provisioner selects the profile for which they want to delete accounts.
- *"Define the IdentityMap Screen Presentation for the Delete Action" on page 110* describes how to set up a form that controls the appearance of the Select Accounts to Delete form presented to the provisioner.
- *"Specify Unique Resource Data Fields for the Target" on page 111* describes how to set up a form the provisioner completes that specifies the fields and possible default values, used when deleting a template account.

The following instructions describe how to modify the settings in the CourionSuper-User workflow. If you have created a new workflow by copying CourionSuper-User, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the Delete Resources Action

To modify the Properties for Delete Action Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **DELETE** from the **ACTION** drop-down menu.
4. Click on **DELETE REQUEST**.
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Delete**.
4. Click the icon next to **Properties**.

The steps to set up a Properties Form for the Delete action of the Super-User workflow is the same as for the Disable action in this workflow. Follow the instructions provided in *"Configure Properties for the Disable Resources Action" on page 101*

Refine the List of Displayed Provisionee Profiles

In the Delete action of the Super-User workflow, the provisionee is the user for whom you want to delete accounts.

By default, AccountCourier displays all the user account records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of accounts can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Provisionee Search screen (*Figure 43*). The provisioner enters values for one or more fields and AccountCourier searches the community and returns a list of accounts that meet the Provisionee Refine Search criteria. The provisioner then selects an account from the list for which accounts are added.

The provisioner can choose to skip entering data on the Provisionee Search screen. If the screen is skipped, AccountCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Provisionee Search screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the navigation bar.
4. Click on **Delete Request** and click on **Provisionee Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions** and expand **Delete**.
4. Click the icon next to **Provisionee Refine Search**.

The process to refine the list of displayed profiles from a Provisionee Community in the Delete action of the Super-User workflow is the same as in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

Define a Provisionee Community

In the Delete action of the Super-User workflow, the provisionee is the user for whom you want to delete accounts. The Provisionee Community consists of the account records in Active Directory.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the **Action** drop-down menu.
4. Click on **Delete Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Provisionee Community**.

   The process to define the Provisionee Community in the Delete action of the Super-User workflow is the same as in the Change action. See *"Define a Provisionee Community" on page 85* for information about how to complete this form.

Define the IdentityMap Screen Presentation for the Delete Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Delete screen, shown in *Figure 49*.

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the navigation bar.
4. Click on **Delete Request** and click on **IdentityMap Screen**.

Tree View

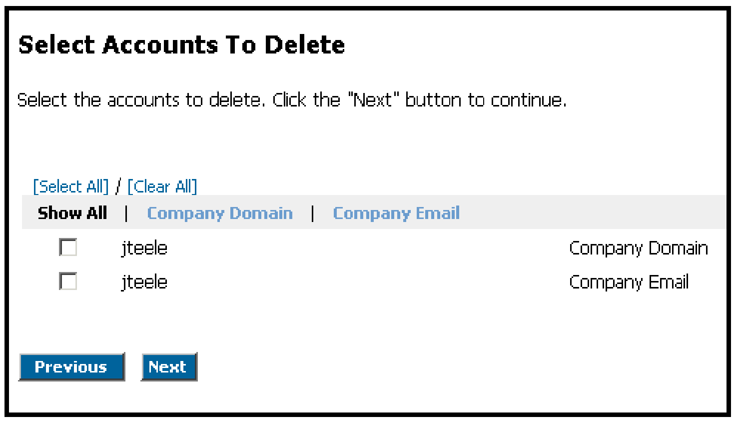
1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **Delete**, expand **Action Settings**, and click the icon next to **IdentityMap Screen**.

The process to modify the fields for the IdentityMap Screen in the Delete action of the Super-User workflow is the same as for a Change action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

The names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. For each target, the provisioner must select the target by checking the checkbox, if they want to delete that target.

Figure 49: Select Accounts to Delete Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are displayed to the provisioner. For the purpose of deleting an account, most targets do not expose any attributes. However, depending on the target, some attributes may be available. For example, some targets provide an attribute for comments, which can be used to document the reason for the account delete action.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the **Action** drop-down menu.
4. Click on **Delete Request**.
5. Click on **Unique Resource Data.**

Tree View

1. Log in to the Administration Manager Tree View.

2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **DELETE**.
4. Click the icon next to **UNIQUE RESOURCE DATA**.

Click on Modify to access the individual attributes and determine which are exposed to the provisioner.

The steps to complete the Unique Target Data Form to Delete a resource are the same as to create a resource. Follow the instructions provided in *"Specify Unique Resource Data Fields for the Target" on page 74*.

Viewing Account Information

This section describes how to configure the View action using the CourionSuper-User sample workflow. This action enables a provisioner to view specified attributes for a provisionee's accounts.

With this workflow, a provisioner selects a provisionee, and then chooses which of the provisionee's accounts to view. The Super-User workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing provisionee.
3. Select the provisionee's accounts to view. The provisioner can only view the attributes for a target that you have configured to display.

The following sections describe configuration of the forms needed for the View action:

- *"Configure Properties for the View Resources Action" on page 113* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 115* describes how to set up a form the provisioner can complete to filter the accounts available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 116* describes how to set up a form that displays the available profiles. The provisioner selects the profile for which they want to view accounts.
- *"Resource Data Selection" on page 117* describes how to set up a form that determines which attributes are displayed for each target.
- *"Worksheet Configuration" on page 120* describes how to specify the sub-worksheets that comprise the sections of the main worksheet on the View action form.
- *"Resource Data Selection Worksheet" on page 122* describes the worksheet displayed to the provisioner.

The following instructions describe how to modify the settings in the CourionSuper-User workflow. If you have created a new workflow by copying CourionSuper-User, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the View Resources Action

To modify the Properties for View Action Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **VIEW** from the **ACTION** drop-down menu.
4. Click on **VIEW REQUEST**.

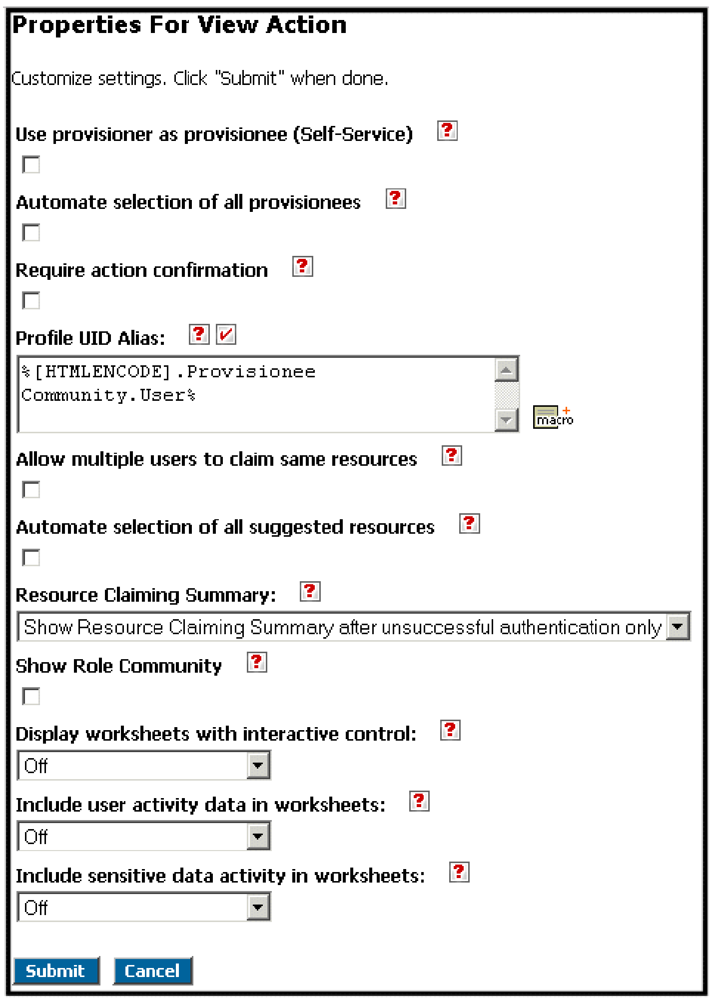
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **VIEW**.
4. Click the icon next to **PROPERTIES**.

The Administration Manager displays the Properties for View Action Form, shown in *Figure 50*.

Figure 50: Properties for View Action



5. Leave the **USE PROVISIONER AS PROVISIONEE (SELF-SERVICE)** checkbox unchecked, since it does not apply in this workflow.
6. Select the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox to enable automatic selection of the provisionee profile (and to bypass the Provisionee Community screen) when only a single provisionee profile is retrieved from the connector. This setting is not selected by default.

   In the Super-User workflow, the provisionee is the user for whom you want to view account attributes. Therefore, if this field is selected it would be necessary to authenticate into the workflow with the user's account name and password. So it is likely you will not want to select this field.

7. Select the **REQUIRE ACTION CONFIRMATION** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.
8. The **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the CourionSuper-User sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
9. Leave the **ALLOW MULTIPLE USERS TO CLAIM SAME RESOURCES** and **AUTOMATE SELECTION OF ALL SUGGESTED RESOURCES** checkboxes unchecked since this workflow does not use resource claiming.
10. Leave the **RESOURCE CLAIMING SUMMARY** option set to "Show Resource Claiming Summary after unsuccessful authentication only".
11. Leave the **SHOW ROLE COMMUNITY** checkbox unchecked since the Super-User workflow does not use the role community.
12. **DISPLAY ADVANCED WORKSHEETS** — Note: This feature is no longer supported.
13. **INCLUDE USER ACTIVITY DATA IN WORKSHEETS** — Select one of the following options to determine whether the worksheet displays data from targets designated as having **USER ACTIVITY** capability. The target capability is displayed on the Target Configuration Form. For details on capabilities, see the chapter "Configure Global Actions and Settings" in the manual *Configuring Workflows with the Access Assurance Suite™ Administration Manager*. You set the capability of a target within the file `feature_extensions.xml`, located in

    Program Files\Courion Corporation\CourionService\conf\

    FORCE — Select a value of **ON** to always include user activity data in the worksheet. Select a value of **OFF** to always exclude user activity data.

    CONDITIONAL — You can choose whether to include user activity data based on a set of conditions. You define conditions with the Create Conditions form. For details on defining conditions, see the manual *Configuring Workflows with the Access Assurance Suite™ Administration Manager*.
14. **INCLUDE SENSITIVE DATA ACTIVITY IN WORKSHEETS** — Select one of the following options to determine whether the worksheet displays data from targets designated as having **SENSITIVE DATA** capability. As with the **USER ACTIVITY** capability, you set the capability of a target within the file `feature_extensions.xml`

    FORCE — Select a value of **ON** to always include sensitive data activity in the worksheet. Select a value of **OFF** to always exclude sensitive data activity.

    CONDITIONAL — You can choose whether to include sensitive data activity based on a set of conditions. You define conditions with the Create Conditions form. For details on defining conditions, see the manual *Configuring Workflows with the Access Assurance Suite™ Administration Manager*.
15. Click **SUBMIT**.

Refine the List of Displayed Provisionee Profiles

In the View action of the Super-User workflow, the provisionee is the user for whom you want to view account information.

By default, AccountCourier displays all the user account records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of accounts can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Provisionee Search screen (*Figure 43*). The provisioner enters values for one or more fields and AccountCourier searches the community and returns a list of accounts that meet the Provisionee Refine Search criteria. The provisioner then selects an account from the list for which accounts are added.

The provisioner can choose to skip entering data on the Provisionee Search screen. If the screen is skipped, AccountCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Provisionee Search screen is not displayed to the provisioner, by unchecking the **ACTIVE** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **VIEW** from the navigation bar.
4. Click on **VIEW REQUEST** and click on **PROVISIONEE REFINE SEARCH**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONSUPER-USER** workflow.
3. Expand **ACTIONS** and expand **VIEW**.
4. Click the icon next to **PROVISIONEE REFINE SEARCH**.

The process to refine the list of displayed profiles from a Provisionee Community in the View action of the Super-User workflow is the same as in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

Define a Provisionee Community

In the View action of the Super-User workflow, the provisionee is the user for whom you want to view account information. The Provisionee Community consists of the account records in Active Directory.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONSUPER-USER** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **VIEW** from the **ACTION** drop-down menu.
4. Click on **VIEW REQUEST**.
5. Click on **PROVISIONEE COMMUNITY**.

Note: You can also access the Provisionee Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Provisionee Community**.

   The process to define the Provisionee Community in the View action of the Super-User workflow is the same as in the Change action. See *"Define a Provisionee Community" on page 85* for information about how to complete this form.

Resource Data Selection

The Resource Data Selection form displays information associated with each target resource. For each target you choose which attributes to display.

To set up the Resource Data Selection Form:

Flowchart View

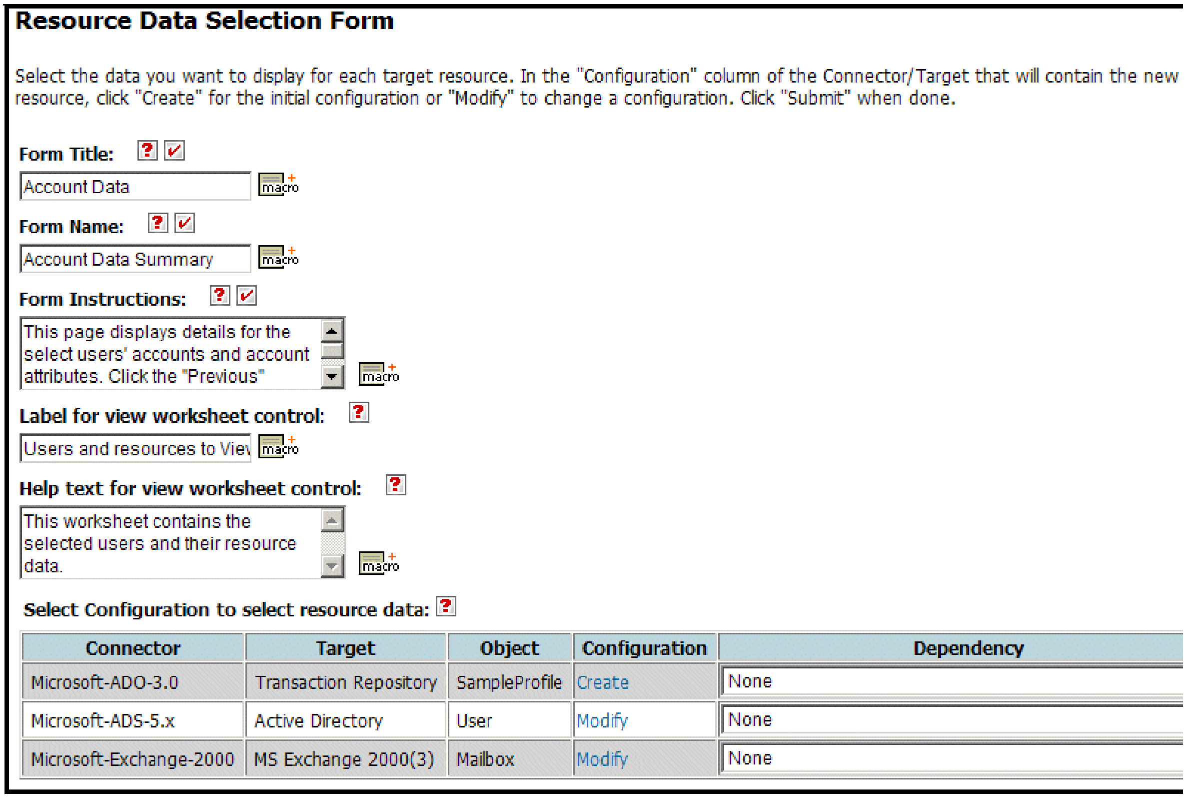
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **View** from the navigation bar.
4. Click on **View Request** and click on **Resource Data Selection**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **View**, expand **Action Settings** and click the icon next to **Resource Data Selection.**

   The Administration Manager displays the Resource Data Selection Form shown in *Figure 51*.

Figure 51: Resource Data Selection Form (a)



Resource Data Selection Form

Select the data you want to display for each target resource. In the "Configuration" column of the Connector/Target that will contain the new resource, click "Create" for the initial configuration or "Modify" to change a configuration. Click "Submit" when done.

Form Title:
Account Data

Form Name:
Account Data Summary

Form Instructions:
This page displays details for the select users' accounts and account attributes. Click the "Previous"

Label for view worksheet control:
Users and resources to Viev

Help text for view worksheet control:
This worksheet contains the selected users and their resource data.

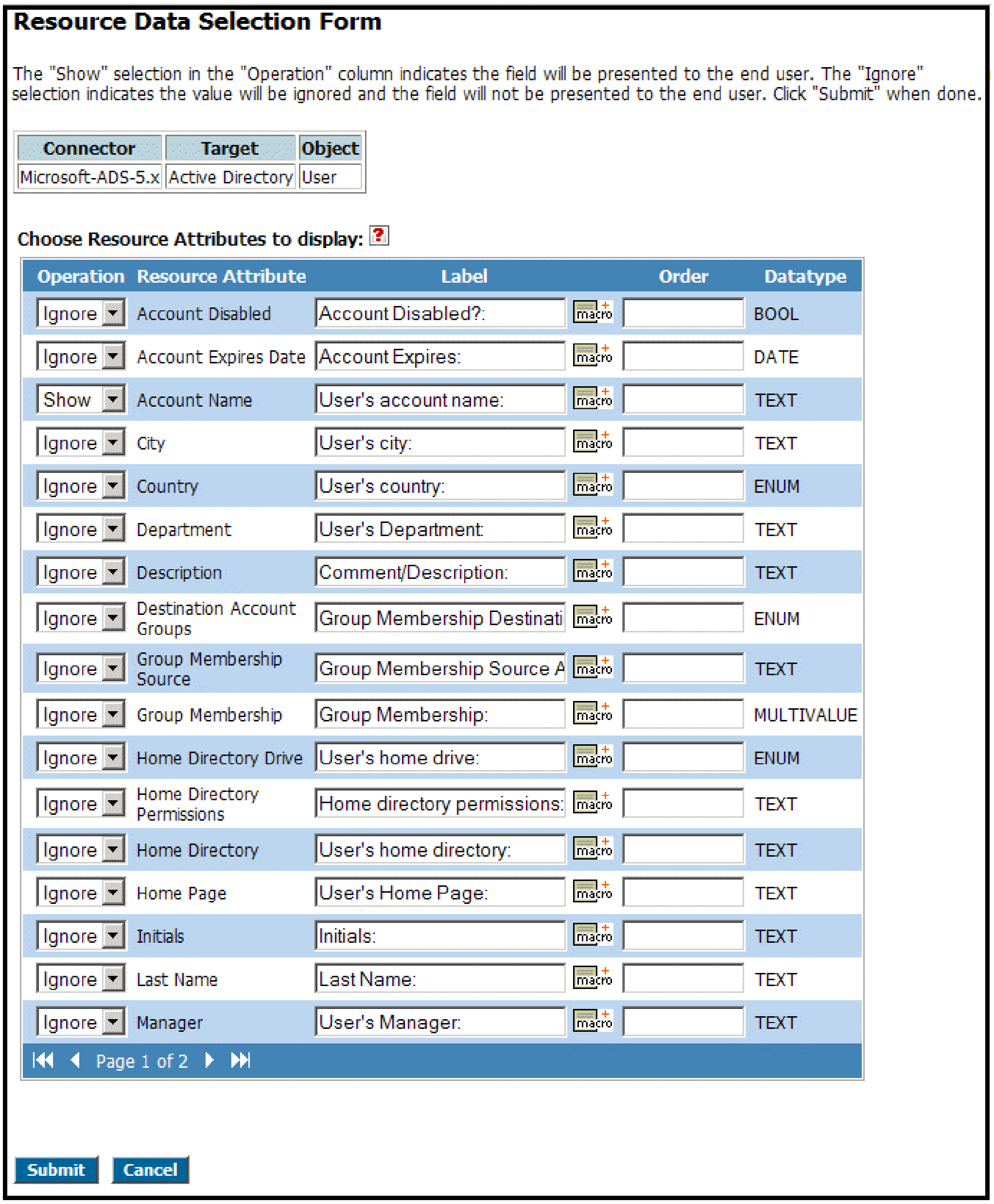
Select Configuration to select resource data:

Connector	Target	Object	Configuration	Dependency
Microsoft-ADO-3.0	Transaction Repository	SampleProfile	Create	None
Microsoft-ADS-5.x	Active Directory	User	Modify	None
Microsoft-Exchange-2000	MS Exchange 2000(3)	Mailbox	Modify	None

4. Text in the **Form Title** text box appears on the title bar of the browser window.
5. Text in the **Form Name** text box identifies the form.
6. Text in the **Form Instructions** text box includes instructions for the provisioner about how to use this form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
7. Text in the **Label for Verification worksheet control** text box identifies the verification report control, which contains the selected users and their resource data.
8. Text in the **Help text for verification report control** text box describes the verification report control.
9. In the **Dependency** column, select the name of the target where the first resource must be successfully processed before any other resources are processed.

   Note: If you want Target C to be dependent on Target A and Target B, make the following dependency: Target C is dependent on Target B, which is dependent on Target A.
10. In the **Configuration** column of the connector/target that contains the data for the resource, click **Create**. If a Resource Data Selection form for this connector/target has already been configured, click **Modify** to change the form. The Resource Data Selection Form for the individual target is displayed, as shown in *Figure 52*. Up to twenty-five attributes for that target are displayed in a table. To view additional attributes, click the “next page” icon at the bottom of the table.

Figure 52: Resource Data Selection Form (b)



Resource Data Selection Form

The "Show" selection in the "Operation" column indicates the field will be presented to the end user. The "Ignore" selection indicates the value will be ignored and the field will not be presented to the end user. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADS-5.x	Active Directory	User

Choose Resource Attributes to display: ?

Operation	Resource Attribute	Label	Order	Datatype
Ignore	Account Disabled	Account Disabled?:		BOOL
Ignore	Account Expires Date	Account Expires:		DATE
Show	Account Name	User's account name:		TEXT
Ignore	City	User's city:		TEXT
Ignore	Country	User's country:		ENUM
Ignore	Department	User's Department:		TEXT
Ignore	Description	Comment/Description:		TEXT
Ignore	Destination Account Groups	Group Membership Destinati		ENUM
Ignore	Group Membership Source	Group Membership Source A		TEXT
Ignore	Group Membership	Group Membership:		MULTIVALUE
Ignore	Home Directory Drive	User's home drive:		ENUM
Ignore	Home Directory Permissions	Home directory permissions:		TEXT
Ignore	Home Directory	User's home directory:		TEXT
Ignore	Home Page	User's Home Page:		TEXT
Ignore	Initials	Initials:		TEXT
Ignore	Last Name	Last Name:		TEXT
Ignore	Manager	User's Manager:		TEXT

Page 1 of 2

Submit Cancel

11. In the **OPERATION** column select **SHOW** to display the attribute on the account data report or **IGNORE** to omit the attribute from the account data report.
12. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner form. You can edit these fields. For example, you could change the “EmployeeBadgeNumber” field to “Badge number:”
13. In the **ORDER** column, enter a number for each selected field to determine the order the field names are listed. The field numbered **0** appears at the top of the list.
14. Click **SUBMIT** to save selections on the Resource Data Selection Form, then click **SUBMIT** on the first Resource Data Selection form.

Worksheet Configuration

Worksheet configuration enables you to specify the sub-worksheets that comprise the sections of the main worksheet on the View action form. Each sub-worksheet represents a condition that is applied to provisionees. These can include conditions that you have defined or the pre-defined conditions included with the Administration Manager. You can choose which of the sub-worksheets to display to the provisioner, along with the order in which they appear. The sub-worksheets display the account attributes selected to **Show** on the Resource Data Selection Form (*Figure 52*).

The Administration Manager includes one pre-defined sub-worksheet that is intended for use with the View action, along with another intended for use with the Verify action. You can create your own conditions that separate provisionees into groups according to your requirements. For example, you might create conditions based on company divisions or locations. You could then create separate workflows to be used for each division or location, thereby limiting the provisionees that can be viewed in each workflow.

If you have created conditions, be sure that you have also defined a sub-worksheet that corresponds to each of the conditions you created. See *"References to Administration Manager Forms" on page 245* for information about how to set up sub-worksheets and conditions.

Flowchart View

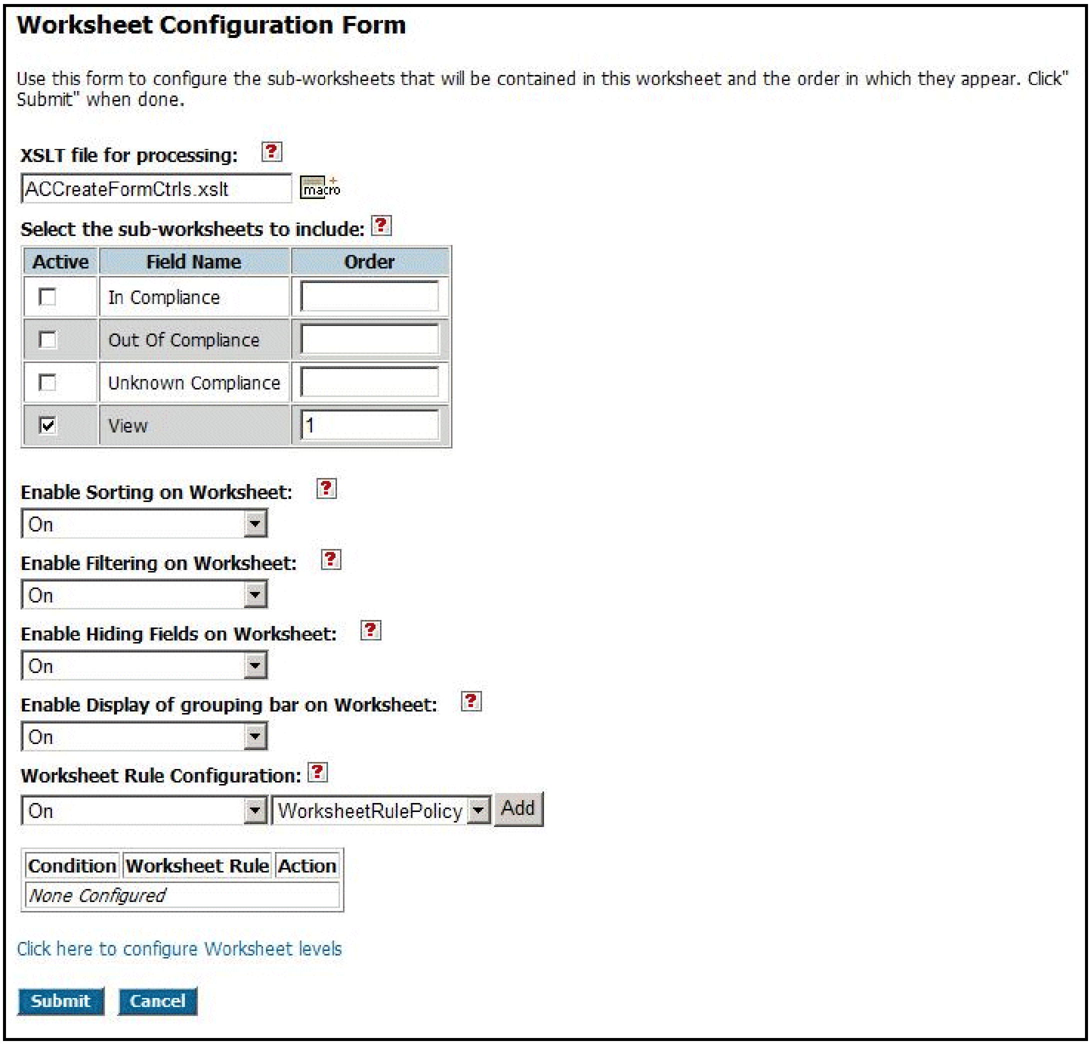
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionSuper-User** from the **Workflow** drop-down menu.
3. Select **Business Process** and **View** from the navigation bar.
4. Click on **View Request** and click on **Worksheet Configuration**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionSuper-User** workflow.
3. Expand **Actions**, expand **View**, and click the icon next to **Worksheet Configuration.**

The Administration Manager displays the Worksheet Configuration Form, shown in *Figure 53*.

Figure 53: Worksheet Configuration Form



4. Specify the file name or a macro that selects the **XSLT File for Processing**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTML controls are rendered, controlling how provisioners interact with the data. The default file for the Super-User workflow is ACCreateFormCtrls.xslt.

   To customize an XSLT file, copy the default file provided by Courion and rename it. Then edit the renamed file as needed and assign that file to this field.

5. Select sub-worksheets based on conditions you have created or the pre-defined conditions. In the default values for the Super-User sample workflow, View is the only appropriate selection, since the other options are used for compliance workflows. In the order column, enter the number that represents the order that the sub-worksheets appear.

6. **Enable Sorting on Worksheet** — Select one of the following options to determine whether the sorting feature is available on the worksheet:

   On - Sorting is available on the worksheet and for the user activity data table. This is the default.

   Off - Sorting is not available on the worksheet or the user activity data table.

CONDITIONAL - Choose whether to make sorting available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

7. **ENABLE FILTERING ON WORKSHEET** — Select one of the following options to determine whether the filtering feature is available on the worksheet:

   ON - Filtering is available on the worksheet or the user activity data table. This is the default.

   OFF - Filtering is not available on the worksheet or the user activity data table. Advanced filtering is not available either.

   CONDITIONAL - Choose whether to make filtering available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

8. **ENABLE HIDING FIELDS ON WORKSHEET** — Select one of the following options to determine whether the hiding fields feature is available on the worksheet:

   ON - Hiding fields is available on the worksheet. This is the default.

   OFF - Hiding fields is not available on the worksheet.

   CONDITIONAL - Choose whether to make hiding fields available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

9. **ENABLE DISPLAY OF GROUPING BAR ON WORKSHEET** — Select one of the following options to determine whether the grouping bar is available on the worksheet:

   ON - The grouping bar is available on the worksheet. This is the default.

   OFF - The grouping bar is not available on the worksheet.

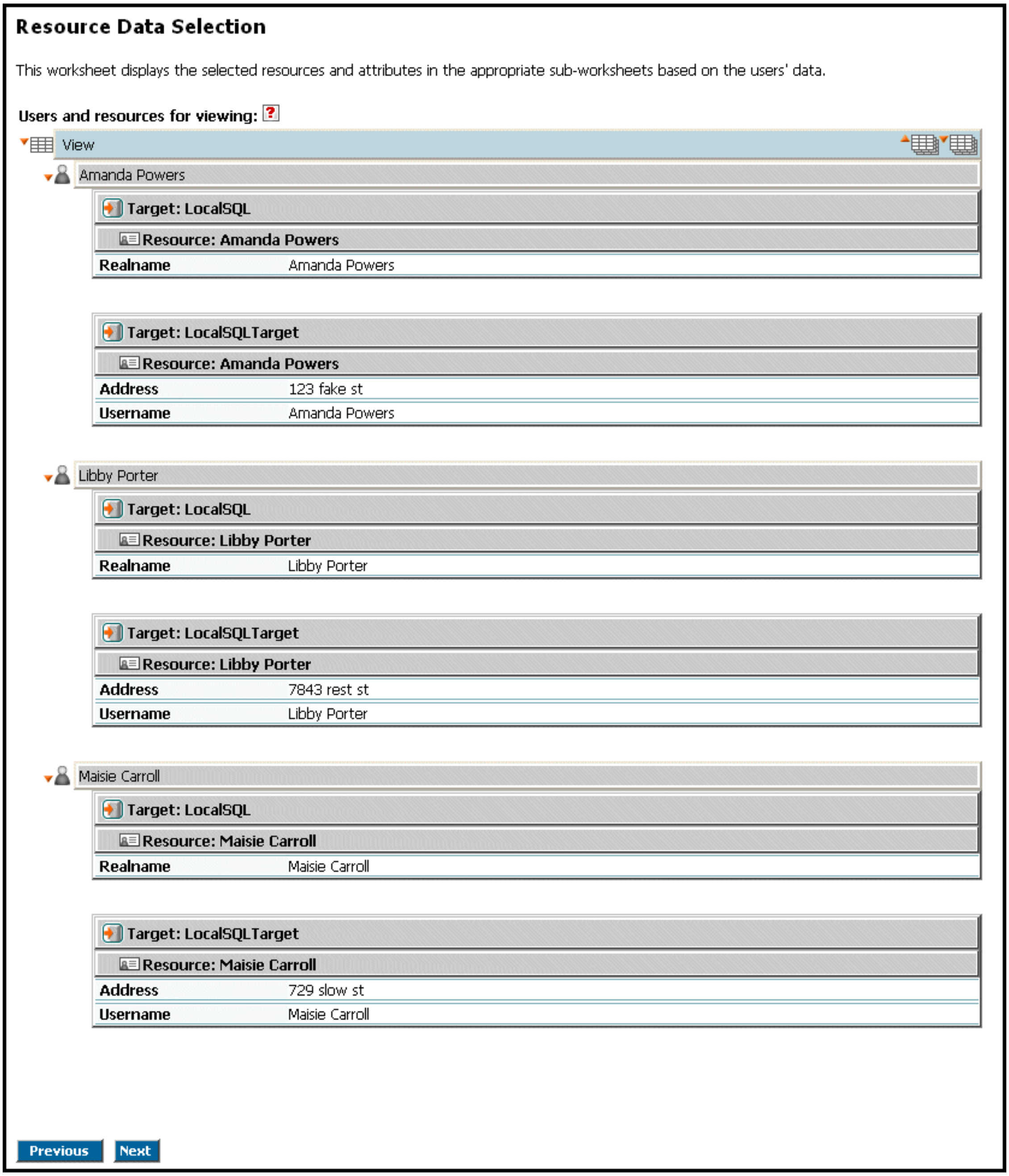
   CONDITIONAL - Choose whether to make the grouping bar available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

10. Click **SUBMIT**.

Resource Data Selection Worksheet

Figure 54 shows an example of the Resource Data Selection worksheet displayed to the provisioner.

Figure 54: Resource Data Selection Screen



If you click on the icon of the person next to the user name, that user's record collapses, hiding the individual attributes. Clicking on the table icons with the up and down arrows collapse or expand all user records for that particular sub-worksheet.

Chapter 7: Configuring a Compliance Workflow

This chapter describes how to configure a workflow that enables a provisioner or administrator to check the compliance status of users, using the CourionCompliance sample workflow as a model. With this workflow, a provisioner can view details of user accounts, grouped according to compliance status. Compliance status is based on a set of conditions or values that can be configured based on company compliance policy. The provisioner can then accept, reject, or mark for further research each user's compliance status. Using an interactive worksheet, the provisioner can filter, sort and reorder the user account data presented in the workflow.

Forms Used by the Compliance Workflow

With this workflow, a provisioner verifies the compliance of users, based on a set of conditions/policies defined within the workflow. The Compliance workflow guides provisioners through the following steps:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select one or more existing users for compliance verification.
3. View the compliance status of the selected users. Details of each user's accounts may be viewed. Account details may be selected on a per user basis.
4. Choose a compliance verification option for each user (Accept, Reject, Change, Research, or other customized value.).

The following sections describe configuration of the forms needed for the Verify action:

- *"Configure the Properties for the Verify Action" on page 126* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 129* describes how to set up a form the provisioner can complete to filter the profiles available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 130* describes how to set up a form that displays the available profiles. The provisioner selects the profile for which they want to add accounts.
- *"Resource Data Selection" on page 134* describes how to set up a form that defines the conditions for compliance for each target.
- *"Worksheet Configuration" on page 139* describes how to set up a form that determines which compliance options are displayed to the provisioner.
- *"ComplianceCourier Worksheets" on page 141* describes the difference between the standard and interactive worksheets displayed to the provisioner.

The following instructions describe how to modify the settings in the CourionCompliance workflow. If you have created a new workflow by copying CourionCompliance, modify the forms in that workflow. See *“Copying Sample Workflows” on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure the Properties for the Verify Action

The ComplianceCourier Verify action enables selected provisioners to verify the validity of user resources and attributes.

To set up the Properties for the Verify Action Form:

Flowchart View

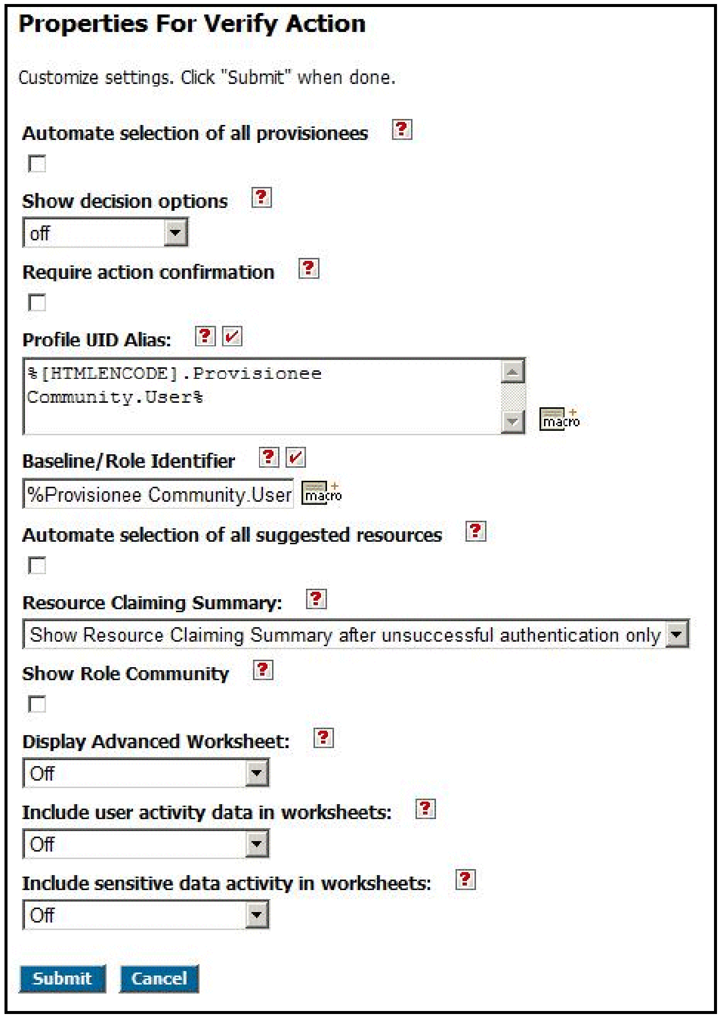
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionCompliance** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Verify** from the navigation bar.
4. Click on **Verify Request** and click on **Properties**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionCompliance** workflow.
3. Expand **Actions**, expand **Verify**, expand **Action Settings**.
4. Click the icon next to **Properties**.

The Administration Manager displays the Properties for Verify Action Form, shown in *Figure 55*.

Figure 55: Properties for the Verify Action Form



5. Select the **AUTOMATE SELECTION OF ALL PROVISIONEES** checkbox if you want to enable automatic selection of all users (and to bypass the Provisionee Community screen). ComplianceCourier automatically selects all provisionees that meet the refined search criteria and includes them in the `%Provisionee Community.User%` macro.

6. **SHOW DECISION OPTIONS** — You can determine the level of detail in which decisions are made. The following options are available:

   Off — No decision options are displayed. You can only view compliance information.

   User Level — Decisions are applied to all accounts associated with the user. This is the default.

   Target Level — Decisions are applied to all accounts associated with the user that are found on the specified target.

   Resource Level — Decisions are applied to each account separately.

   Attribute Level — Decisions are applied to each attribute separately. An attribute will only be available for decisions if the value of the **OPERATION** field on the Resource Data Selection Form is set to **Show** (see *Figure 61*).

   By default the following decisions are available on the provisioner form:

Change — Change the user's compliance status. This selection requires the user to enter text into the Comments section of the form.

Accept — Accept the user's compliance status.

Reject — Reject the user's compliance status.

Research — Research the compliance status (does not alter the status). This selection requires the user to enter text in the Comments section of the form.

To change these defaults, you can modify the `AttestationDecisions.xml` file in the CourionService/AttestationDecisions directory.

Note: If you are using the XML Access option to automate the Verify action, you must set **SHOW DECISION OPTIONS** to **Off**.

7. Select the **REQUIRE ACTION CONFIRMATION** checkbox to have the workflow prompt the provisioner with a confirmation screen. This setting is turned on by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step

8. The **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the CourionCompliance sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.

9. The **BASELINE/ROLE IDENTIFIER** specifies the Profile UID of a provisionee or category of user to compare against in the verify action.

   In many of the sample workflows, the default macro for this field is "%Provisionee Community.User%", which will display the unique identifier of the provisionee.

   If you wanted to specify that the baseline that users are compared to is dependent on their job title, then you could:

   a. Create a custom macro, BaselineTemplate which has the following native query string:

      ```
      SELECT ProfileUID FROM Baseline WHERE Title = '%Custom
      Macro.DestUserTitle%'
      ```

      where the custom macro "DestUserTitle" would get the title of the user based on their PROFILE UID. The Baseline table would contain a list of all possible job titles and a corresponding PROFILEUID to be used for the baseline

   b. Specify `%Custom Macro.BaselineTemplate%` as the value for Baseline/ Role Identifier.

   You can use a literal value such as "Sales Manager," or create a custom macro that resolves to a category of user with the characteristics you want the verify action to compare against. For example:

   ```
   %Custom Macro.Get_RoleID_Based_On_Auth_Step_1_BadgeNumber%
   ```

10. Select the **AUTOMATE SELECTION OF ALL SUGGESTED RESOURCES** checkbox to enable automatic selection of the resources suggested for the user or users (and to bypass the Resource List screen).

11. Leave the **RESOURCE CLAIMING SUMMARY** option set to "Never show resource claiming summary" since this workflow does not use resource claiming.

12. Leave the **SHOW ROLE COMMUNITY** checkbox unchecked since the CourionCompliance workflow does not use the role community.

13. **DISPLAY ADVANCED WORKSHEETS** — Note: This feature is no longer supported.

14. **INCLUDE USER ACTIVITY DATA IN WORKSHEETS** — Select one of the following options to determine whether the worksheet displays data from targets designated as having **USER ACTIVITY** capability. The target capability is displayed on the

Target Configuration Form. For details on capabilities, see the chapter “Configure Global Actions and Settings” in the manual *Configuring Workflows with the Access Assurance Suite™ Administration Manager*. You set the capability of a target within the file `feature_extensions.xml`, located in

Program Files\Courion Corporation\CourionService\conf\

FORCE — Select a value of **ON** to always include user activity data in the worksheet. Select a value of **OFF** to always exclude user activity data.

CONDITIONAL — You can choose whether to include user activity data based on a set of conditions. You define conditions with the Create Conditions form. For details on defining conditions, see the manual *Configuring Workflows with the Access Assurance Suite™ Administration Manager*.

15. **INCLUDE SENSITIVE DATA ACTIVITY IN WORKSHEETS** — Select one of the following options to determine whether the worksheet displays data from targets designated as having **SENSITIVE DATA** capability. As with the **USER ACTIVITY** capability, you set the capability of a target within the file `feature_extensions.xml`

    FORCE — Select a value of **ON** to always include sensitive data activity in the worksheet. Select a value of **OFF** to always exclude sensitive data activity.

    CONDITIONAL — You can choose whether to include sensitive data activity based on a set of conditions. You define conditions with the Create Conditions form. For details on defining conditions, see the manual *Configuring Workflows with the Access Assurance Suite™ Administration Manager*.

16. Click **SUBMIT**.

Refine the List of Displayed Provisionee Profiles

By default, ComplianceCourier displays all the profiles to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the community of users can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Provisionee Search screen (*Figure 56*). The provisioner enters values for one or more fields and ComplianceCourier searches the community and returns a list of profiles that meet the Provisionee Refine Search criteria. The provisioner then selects a profile from the list of resources to change.

The provisioner can choose to skip entering data on this form. If the form is skipped, ComplianceCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Provisionee Search screen is not displayed to the provisioner, by unchecking the **ACTIVE** checkbox for all search fields.

To set up the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONCOMPLIANCE** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **VERIFY** from the navigation bar.
4. Click on **VERIFY REQUEST** and click on **PROVISIONEE REFINE SEARCH**.

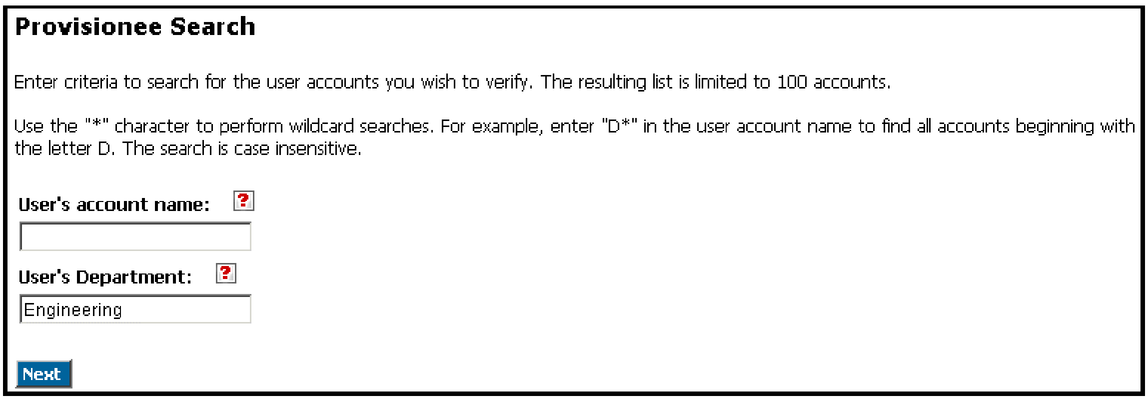
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionCompliance** workflow.
3. Expand **Actions**, expand **Verify**, expand **Action Settings**, and click the icon next to **Provisionee Refine Search**.

The process to refine the list of displayed profiles from a Provisionee Community in the Verify action of the Compliance workflow is the same as in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

Figure 56 shows the screen displayed to provisioner, based on the settings from the Compliance workflow.

Figure 56: Provisionee Search Screen



Define a Provisionee Community

In the Compliance workflow, the provisionee is the user for whom you want to verify compliance information. The Provisionee Community consists of user records in Active Directory.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **CourionCompliance** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Verify** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

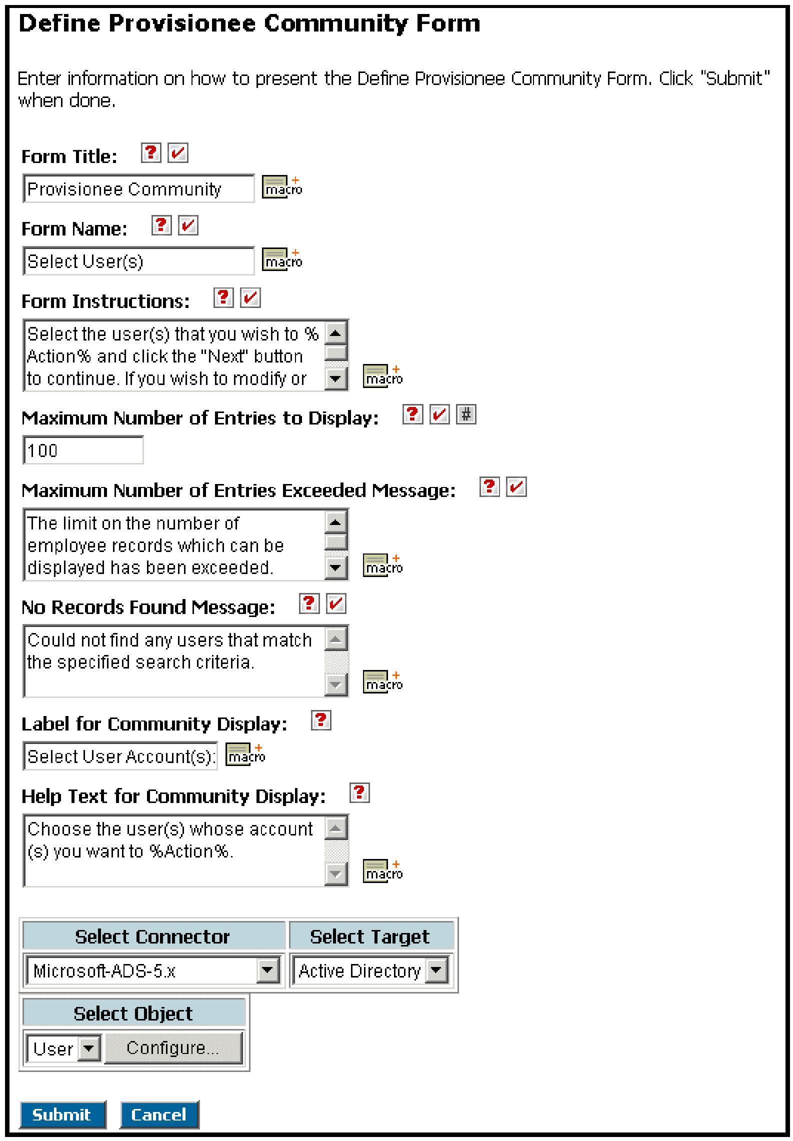
1. Log in to the Administration Manager Flowchart View.
2. Select **CourionCompliance** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **CourionCompliance** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Provisionee Community**.

   The Administration Manager displays the Define Provisionee Community Form, shown in *Figure 57* with default text and sample data. You can edit all text boxes.

Figure 57: Define Provisionee Community Form



Define Provisionee Community Form

Enter information on how to present the Define Provisionee Community Form. Click "Submit" when done.

Form Title:
Provisionee Community

Form Name:
Select User(s)

Form Instructions:
Select the user(s) that you wish to %Action% and click the "Next" button to continue. If you wish to modify or

Maximum Number of Entries to Display:
100

Maximum Number of Entries Exceeded Message:
The limit on the number of employee records which can be displayed has been exceeded.

No Records Found Message:
Could not find any users that match the specified search criteria.

Label for Community Display:
Select User Account(s):

Help Text for Community Display:
Choose the user(s) whose account (s) you want to %Action%.

Select Connector	Select Target
Microsoft-ADS-5.x	Active Directory

Select Object	
User	Configure...

Submit Cancel

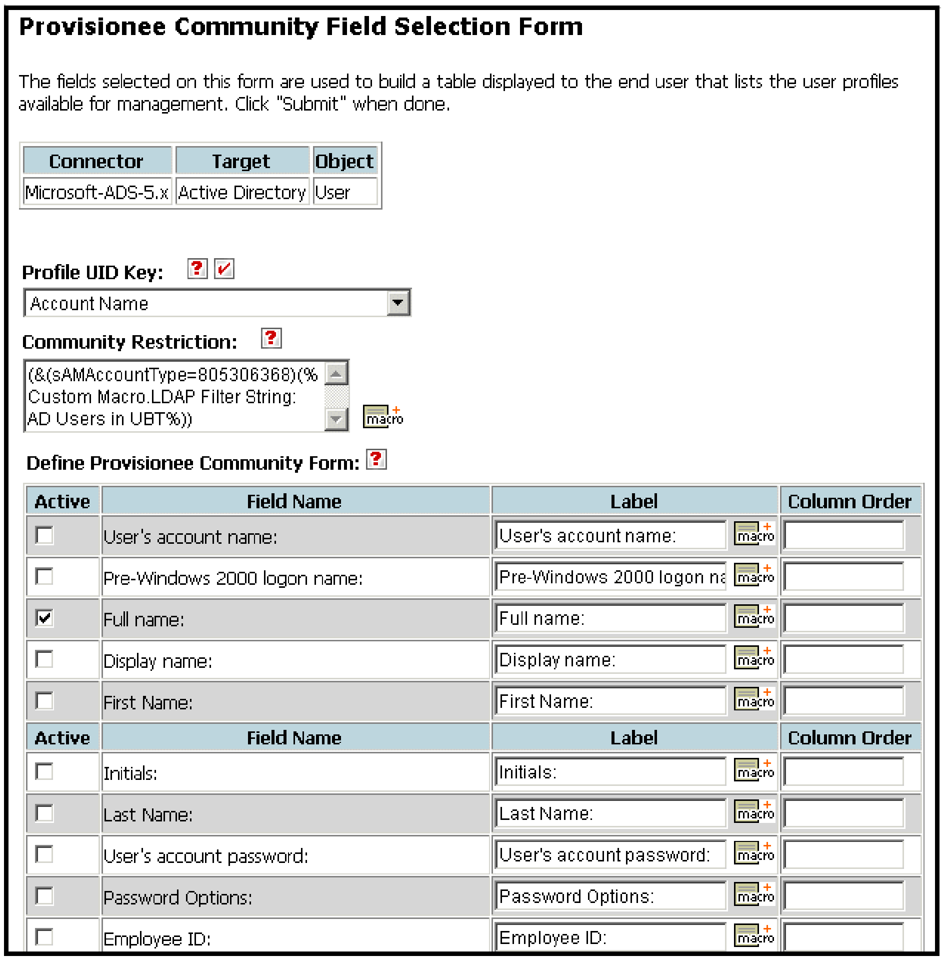
5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.
7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)

8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Provisionee Refine Search Form, can help the provisioner limit the number of returned profiles (see *"Refine the List of Displayed Provisionee Profiles" on page 129*).
9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Provisionee Refine Search Form to display profiles that more closely match search criteria.
10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message appears if the provisioner has entered values on the Provisionee Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Provisionee Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label for Community Display** text box appears as a title over the Mining Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Leave the **Select Connector** drop-down list box set to Microsoft-ADS-5.x, the **Select Target** drop-down list box set to Active Directory, and the **Object** drop-down list box set to User.
14. Click **Configure...**.

    The Administration Manager displays the Define Provisionee Community Field Selection Form, shown in *Figure 58*.

    Note: The list of fields has been shortened to save space.

Figure 58: Define Provisionee Community Field Selection Form



Provisionee Community Field Selection Form

The fields selected on this form are used to build a table displayed to the end user that lists the user profiles available for management. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADS-5.x	Active Directory	User

Profile UID Key:

Account Name

Community Restriction:

(&(sAMAccountType=805306368)(%
Custom Macro.LDAP Filter String:
AD Users in UBT%))

Define Provisionee Community Form:

Active	Field Name	Label	Column Order
☐	User's account name:	User's account name:	
☐	Pre-Windows 2000 logon name:	Pre-Windows 2000 logon na	
☑	Full name:	Full name:	
☐	Display name:	Display name:	
☐	First Name:	First Name:	
Active	**Field Name**	**Label**	**Column Order**
☐	Initials:	Initials:	
☐	Last Name:	Last Name:	
☐	User's account password:	User's account password:	
☐	Password Options:	Password Options:	
☐	Employee ID:	Employee ID:	

15. In the **PROFILE UID KEY** drop-down box, select the unique user ID field in this object that will serve as a link to a user's entries, identified by the Profile UID field, in the Resource Community table.

16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Statement syntax depends on the target datasource. Do not use hashed or encrypted fields in the statement.

    In the Compliance workflow, the macro restricts return of available profiles to Active Directory records that belong to users, and only those users with a profile stored in the IdentityMap.

    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on Defining a Dynamic Community.

17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner.

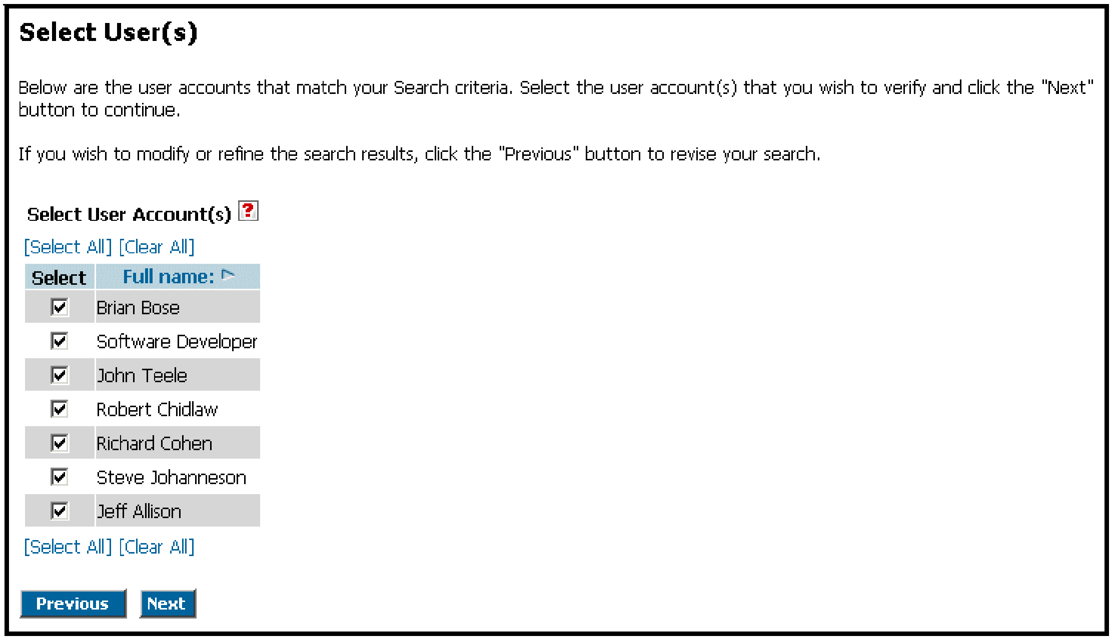
18. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change an "EmployeeBadgeNumber" field to "Badge number:".

19. In the **COLUMN ORDER** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered "1" appears as the first column.

20. Click **SUBMIT**.

Figure 59 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 59: Select User Screen



Resource Data Selection

The Resource Data Selection form displays information associated with each target resource. For each target you choose which attributes to display and then configure specific attributes for a baseline comparison against a default value or condition. The result of the comparison determines if the target is in or out of compliance.

To set up the Resource Data Selection Form:

Flowchart View

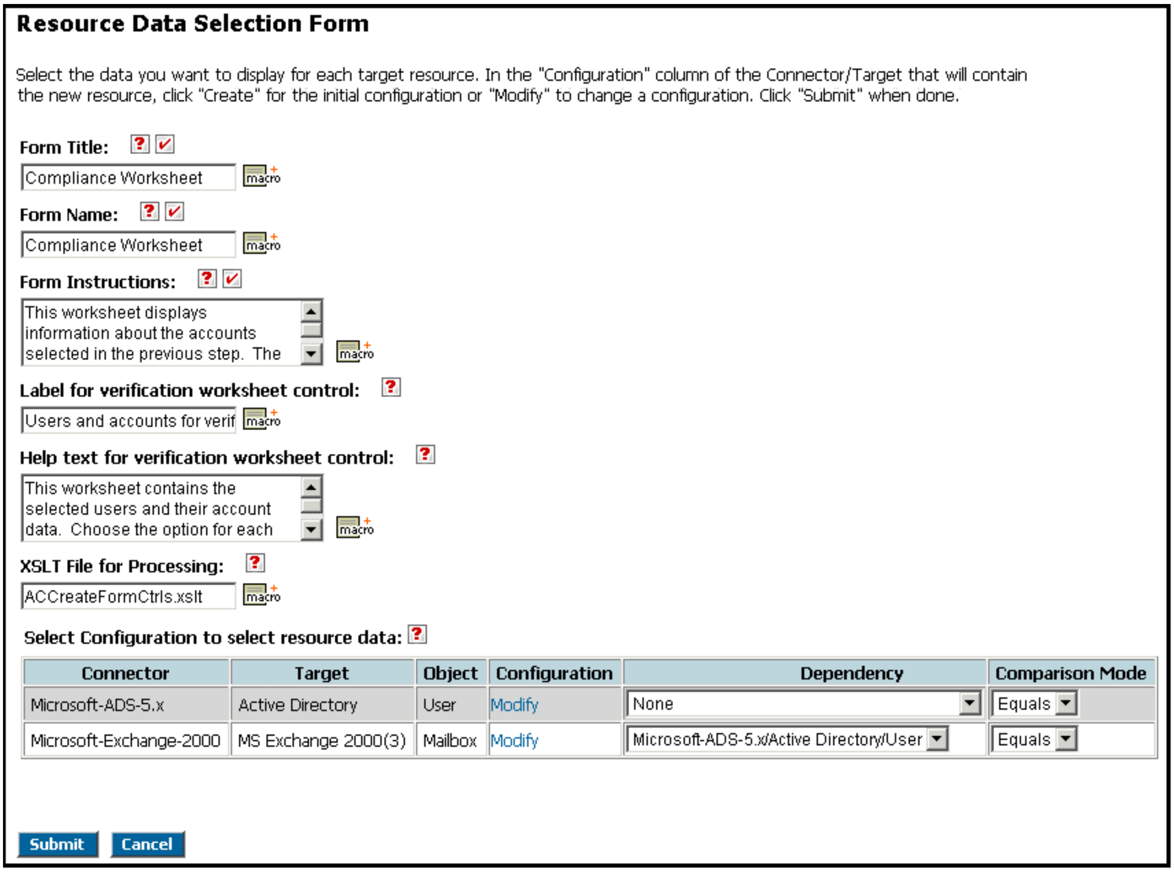
1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONCOMPLIANCE** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **VERIFY** from the navigation bar.
4. Click on **VERIFY REQUEST** and click on **RESOURCE DATA SELECTION**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONCOMPLIANCE** workflow.
3. Expand **ACTIONS**, expand **VERIFY**, expand **ACTION SETTINGS** and click the icon next to **RESOURCE DATA SELECTION.**

   The Administration Manager displays the Resource Data Selection Form shown in *Figure 60*.

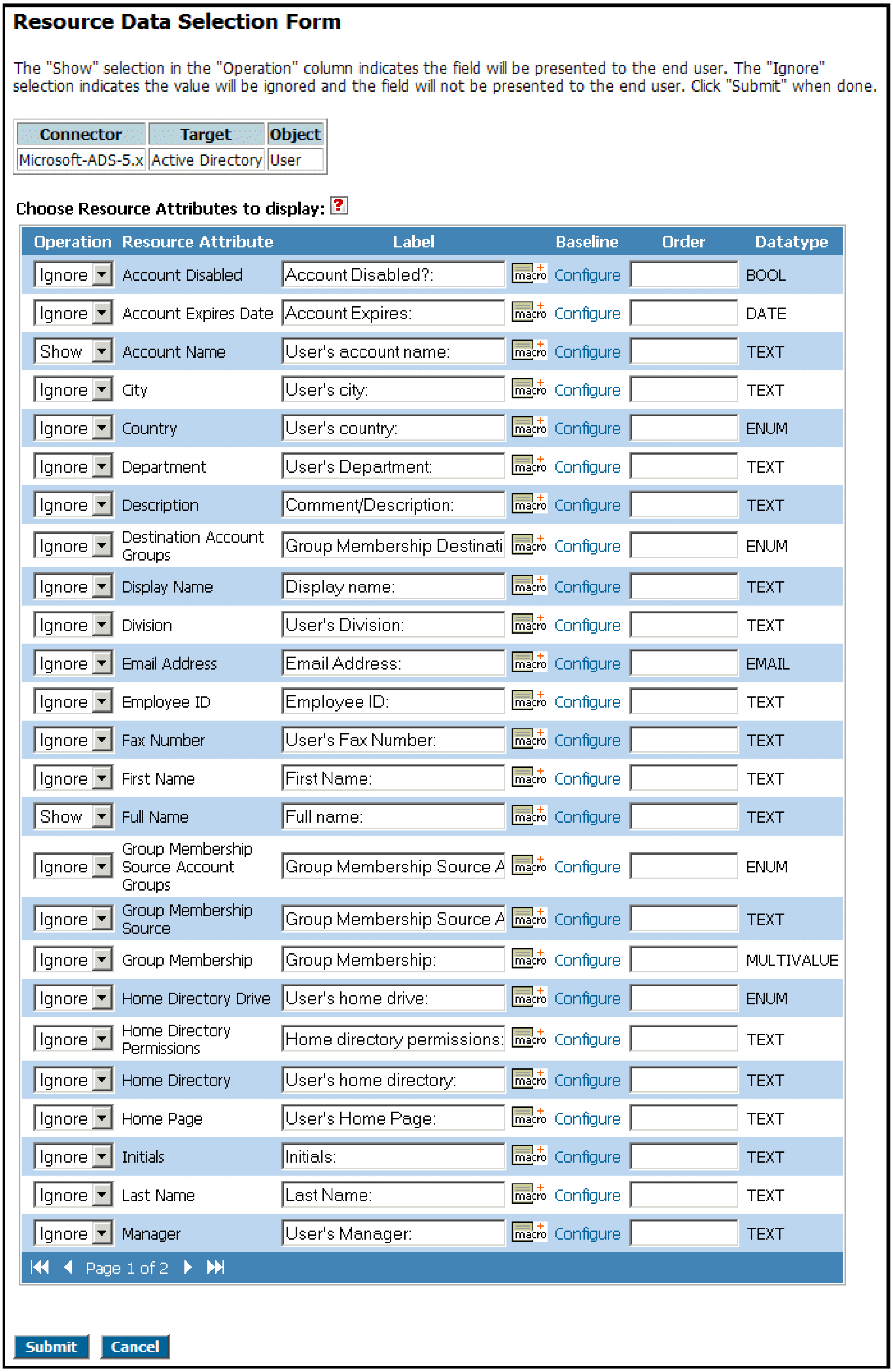
Figure 60: Resource Data Selection Form (a)



4. Text in the **FORM TITLE** text box appears on the title bar of the browser window.
5. Text in the **FORM NAME** text box identifies the form.
6. Text in the **FORM INSTRUCTIONS** text box includes instructions for the provisioner about how to use this form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
7. Text in the **LABEL FOR VERIFICATION WORKSHEET CONTROL** text box identifies the verification report control, which contains the selected users and their resource data.
8. Text in the **HELP TEXT FOR VERIFICATION REPORT CONTROL** text box describes the verification report control.
9. If there is more than one target, in the **DEPENDENCY** column, select the name of the target where the first resource must be successfully processed before any other resources are processed.

   Note: If you want Target C to be dependent on Target A and Target B, make the following dependency: Target C is dependent on Target B, which is dependent on Target A.
10. In the **CONFIGURATION** column of the connector/target that will contain the data for the resource, click **CREATE**. If a Resource Data Selection form for this connector/target has already been configured, click **MODIFY** to change the form. The Resource Data Selection Form for the individual target is displayed, as shown in *Figure 61*. Up to twenty-five attributes for that target are displayed in a table. To view additional attributes, click the “next page” icon at the bottom of the table.

Figure 61: Resource Data Selection Form (b)



Resource Data Selection Form

The "Show" selection in the "Operation" column indicates the field will be presented to the end user. The "Ignore" selection indicates the value will be ignored and the field will not be presented to the end user. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADS-5.x	Active Directory	User

Choose Resource Attributes to display:

Operation	Resource Attribute	Label		Baseline	Order	Datatype
Ignore	Account Disabled	Account Disabled?:	macro	Configure		BOOL
Ignore	Account Expires Date	Account Expires:	macro	Configure		DATE
Show	Account Name	User's account name:	macro	Configure		TEXT
Ignore	City	User's city:	macro	Configure		TEXT
Ignore	Country	User's country:	macro	Configure		ENUM
Ignore	Department	User's Department:	macro	Configure		TEXT
Ignore	Description	Comment/Description:	macro	Configure		TEXT
Ignore	Destination Account Groups	Group Membership Destinati	macro	Configure		ENUM
Ignore	Display Name	Display name:	macro	Configure		TEXT
Ignore	Division	User's Division:	macro	Configure		TEXT
Ignore	Email Address	Email Address:	macro	Configure		EMAIL
Ignore	Employee ID	Employee ID:	macro	Configure		TEXT
Ignore	Fax Number	User's Fax Number:	macro	Configure		TEXT
Ignore	First Name	First Name:	macro	Configure		TEXT
Show	Full Name	Full name:	macro	Configure		TEXT
Ignore	Group Membership Source Account Groups	Group Membership Source A	macro	Configure		ENUM
Ignore	Group Membership Source	Group Membership Source A	macro	Configure		TEXT
Ignore	Group Membership	Group Membership:	macro	Configure		MULTIVALUE
Ignore	Home Directory Drive	User's home drive:	macro	Configure		ENUM
Ignore	Home Directory Permissions	Home directory permissions:	macro	Configure		TEXT
Ignore	Home Directory	User's home directory:	macro	Configure		TEXT
Ignore	Home Page	User's Home Page:	macro	Configure		TEXT
Ignore	Initials	Initials:	macro	Configure		TEXT
Ignore	Last Name	Last Name:	macro	Configure		TEXT
Ignore	Manager	User's Manager:	macro	Configure		TEXT

Page 1 of 2

Submit Cancel

11. In the **OPERATION** column select **SHOW** to display the attribute on the Verification report or **IGNORE** to omit the attribute from the Verification report.

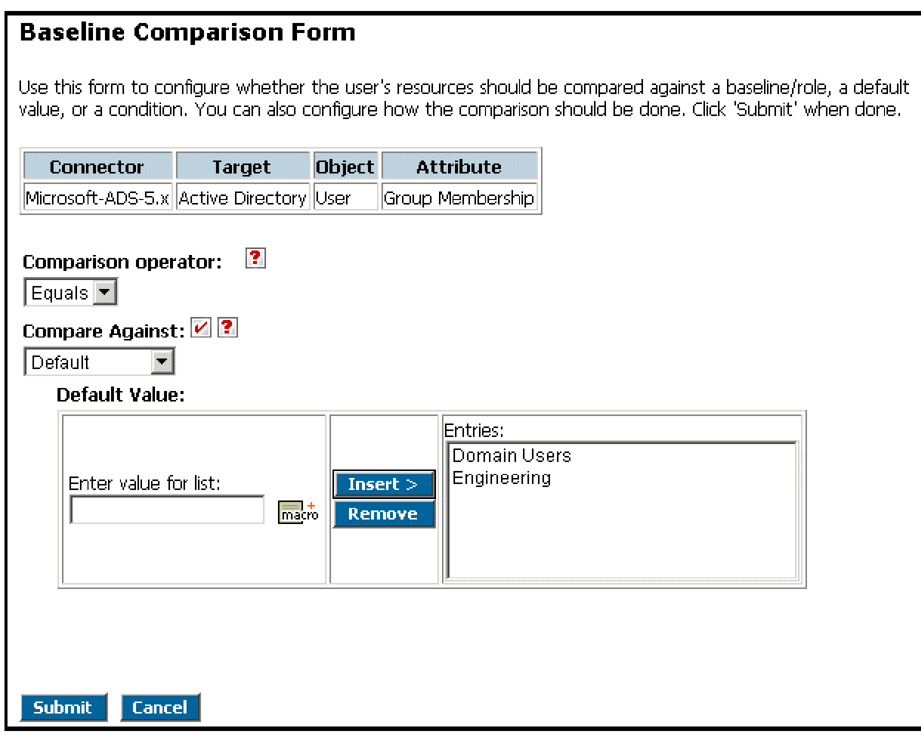
12. The **Label** column displays the field name by default. This text appears next to the associated field input box on the provisioner form. You can edit these fields. For example, you could change the “EmployeeBadgeNumber” field to “Badge number:”
13. In the **Baseline** column, click **Configure** to use this attribute in a comparison against a baseline, role, default value, or condition. When you click **Configure**, the Baseline Comparison Form (*Figure 62*) appears.
14. In the **Order** column, enter a number for each selected field to determine the order the field names are listed. The field numbered **0** appears at the top of the list.
15. Click **Submit** to save selections on the Resource Data Selection Form, then click **Submit** on the first Resource Data Selection form.

The Baseline Comparison Form

ComplianceCourier determines compliance status for the selected users by comparing the value of a specific attribute in a user’s account against the value you configure on the Baseline Configuration Form. You can configure more than one attribute in a target.

You can compare against a default value, condition, or baseline/role value. In the example shown in *Figure 62*, a workflow has been configured to enable an Engineering manager check the group membership of all employees in the engineering department. The Active Directory Group Membership attribute is being compared to a default value of two groups—Domain Users and Engineering. Any users who have additional groups assigned to their Active Directory account are listed as Out of Compliance.

Figure 62: Baseline Comparison Form



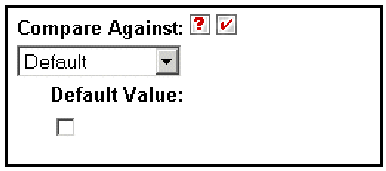
1. The **Compare Against** drop-down box has three possible values—Default, Role/Baseline, and Condition:

- **Default** — The Default Value comparison requires you to specify information determined by the attribute type you have selected. The format of this parameter changes, depending on the type of attribute.

  In the example shown in *Figure 62*, the Group Membership attribute is a multi-value attribute. You add a text string or Macro into the **Enter Value for List** field and click **Insert** to add the value. To remove a value from the **Entries** list, highlight the value and click **Remove**.

  For a Boolean attribute, a checkbox appears on the form, such as that shown in *Figure 63*.

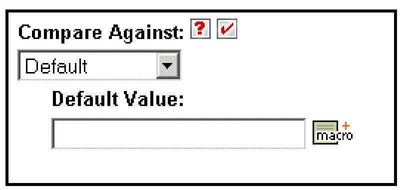
Figure 63: Default Baseline for Boolean Attribute



Check the **Default Value** box to specify that the criteria to compare against is a positive value for that attribute. For example, if you are using the “Accounts Disabled” attribute, checking this box implies that accounts that are disabled are in compliance.

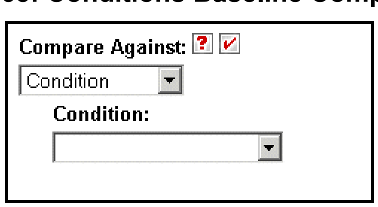
Other attribute types require you to enter a text string or macro that specifies the comparison criteria, such as in *Figure 64*.

Figure 64: Default Baseline for ENUM or TEXT Attribute



- **Baseline/Role** — For this option, ComplianceCourier uses the value of the attribute in the **Baseline/Role Identifier** field you specified in the Properties form as the criteria for comparison. If you assign the `%Role.Community.User%` macro and then configure the Define Role Community Form within this workflow, the baseline comparison is made against the attribute value from a user’s account selected when the workflow is run. For example, instead of comparing against a default set of groups configured in the workflow, as was shown in the example in *Figure 62*, an administrator or manager could select a specific individual or role-based template account and compare against the groups assigned to that account.
- **Condition** — The Condition comparison only appears if the selected attribute is Boolean (a checkbox) and at least one condition has been defined for this workflow. When you select Condition, the Baseline Comparison form displays the Condition drop-down box in *Figure 65*.

Figure 65: Conditions Baseline Comparison



Select a condition that you have already configured from the drop-down list. See *"References to Administration Manager Forms" on page 245* for information about how to set up conditions.

2. Click **SUBMIT**.

Worksheet Configuration

Worksheet configuration enables you to specify the sub-worksheets that comprise the sections of the main worksheet on the Verify action form. Each sub-worksheet represents a condition that is applied to provisionees. These can include conditions that you have defined or the pre-defined conditions included with the Administration Manager. You can choose which of the sub-worksheets to display to the provisioner, along with the order in which they appear. The sub-worksheets display the names of the previously selected provisionees, and require the selection of a verification option for each provisionee, as shown in *Figure 67*.

The Administration Manager includes pre-defined sub-worksheets that correspond to the compliance conditions: In Compliance, Out of Compliance, and Unknown Compliance. These categories, as well as View, appear in the sub-worksheets for the Verify action.

If you have created conditions, be sure that you have also defined a sub-worksheet that corresponds to each of the conditions you created. See *"References to Administration Manager Forms" on page 245* for information about how to set up sub-worksheets and conditions.

Flowchart View

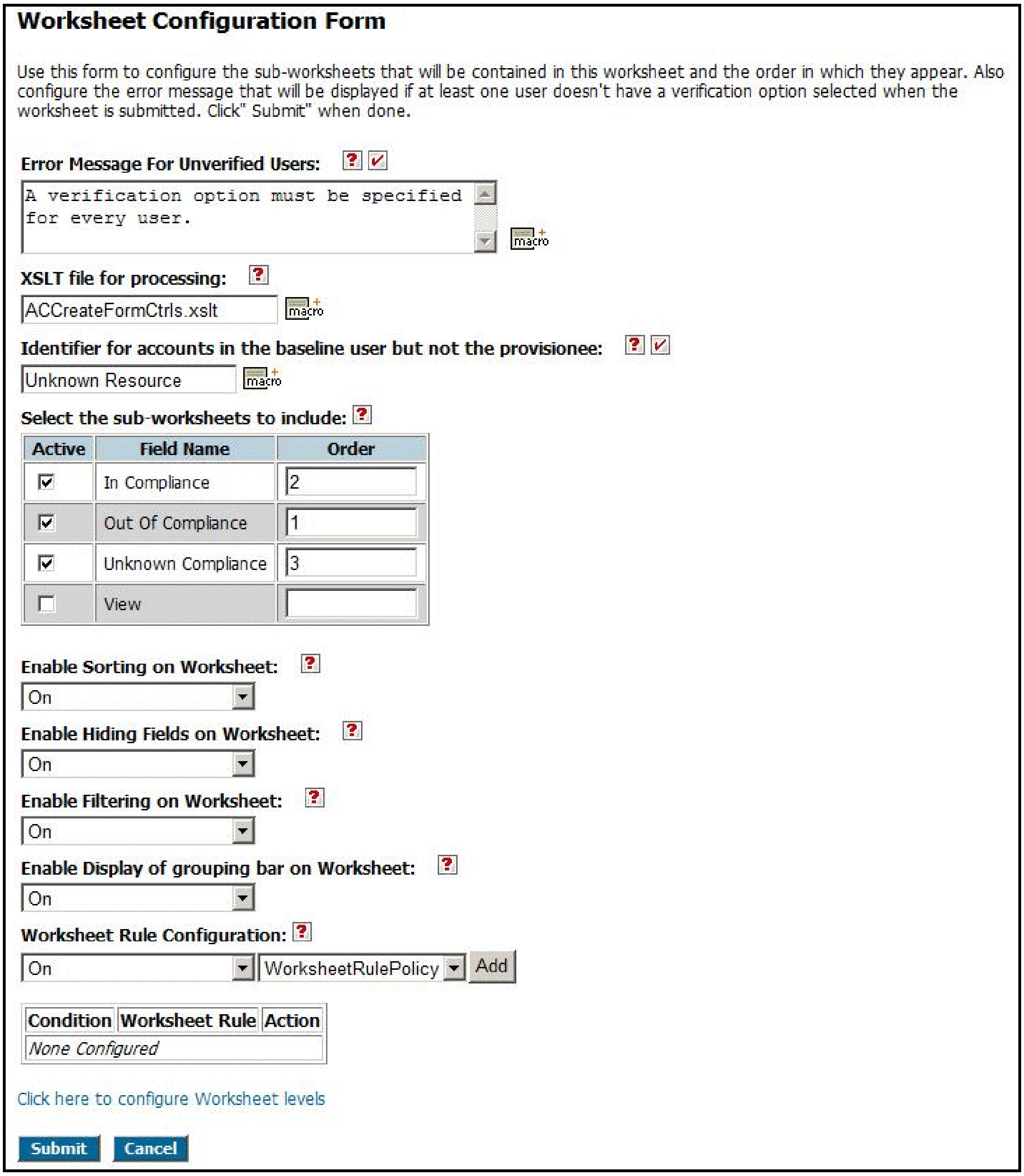
1. Log in to the Administration Manager Flowchart View.
2. Select **COURIONCOMPLIANCE** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **VERIFY** from the navigation bar.
4. Click on **VERIFY REQUEST** and click on **WORKSHEET CONFIGURATION**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURIONCOMPLIANCE** workflow.
3. Expand **ACTIONS**, expand **VERIFY**, and click the icon next to **WORKSHEET CONFIGURATION.**

The Administration Manager displays the Worksheet Configuration Form, shown in *Figure 66*.

Figure 66: Worksheet Configuration Form


Worksheet Configuration Form

Use this form to configure the sub-worksheets that will be contained in this worksheet and the order in which they appear. Also configure the error message that will be displayed if at least one user doesn't have a verification option selected when the worksheet is submitted. Click" Submit" when done.

Error Message For Unverified Users:

A verification option must be specified for every user.

XSLT file for processing:

ACCreateFormCtrls.xslt

Identifier for accounts in the baseline user but not the provisionee:

Unknown Resource

Select the sub-worksheets to include:

Active	Field Name	Order
☑	In Compliance	2
☑	Out Of Compliance	1
☑	Unknown Compliance	3
☐	View	

Enable Sorting on Worksheet:

On

Enable Hiding Fields on Worksheet:

On

Enable Filtering on Worksheet:

On

Enable Display of grouping bar on Worksheet:

On

Worksheet Rule Configuration:

On | WorksheetRulePolicy | Add

Condition	Worksheet Rule	Action
None Configured		

Click here to configure Worksheet levels

Submit Cancel

4. In the **Error Message for Unverified Users** text box, enter a message that will appear to provisioners if they submit a worksheet and at least one user does not have a verification option selected.
5. Specify the file name or a macro that selects the **XSLT File for Processing**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTML controls are rendered, controlling how provisioners interact with the data. The default file for the CourionCompliance workflow is ACCreateFormCtrls.xslt.

   To customize an XSLT file, copy the default file provided by Core Security and rename it. Then edit the renamed file as needed and assign that file to this field.
6. Select sub-worksheets based on conditions you have created or the pre-defined conditions. In the order column, enter the number that represents the order that the sub-worksheets will appear.

7.

8. **ENABLE SORTING ON WORKSHEET** — Select one of the following options to determine whether the sorting feature is available on the worksheet:

   ON - Sorting is available on the worksheet and for the user activity data table. This is the default.

   OFF - Sorting is not available on the worksheet or the user activity data table.

   CONDITIONAL - Choose whether to make sorting available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

9. **ENABLE HIDING FIELDS ON WORKSHEET** — Select one of the following options to determine whether the hiding fields feature is available on the worksheet:

   ON - Hiding fields is available on the worksheet. This is the default.

   OFF - Hiding fields is not available on the worksheet.

   CONDITIONAL - Choose whether to make hiding fields available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

10. **ENABLE FILTERING ON WORKSHEET** — Select one of the following options to determine whether the filtering feature is available on the worksheet:

    ON - Filtering is available on the worksheet or the user activity data table. This is the default.

    OFF - Filtering is not available on the worksheet or the user activity data table. Advanced filtering is not available either.

    CONDITIONAL - Choose whether to make filtering available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

11. **ENABLE DISPLAY OF GROUPING BAR ON WORKSHEET** — Select one of the following options to determine whether the grouping bar is available on the worksheet:

    ON - The grouping bar is available on the worksheet. This is the default.

    OFF - The grouping bar is not available on the worksheet.

    CONDITIONAL - Choose whether to make the grouping bar available on the worksheet based on a set of conditions that you define on the Create Conditions form (see *"Creating Conditions" on page 189*).

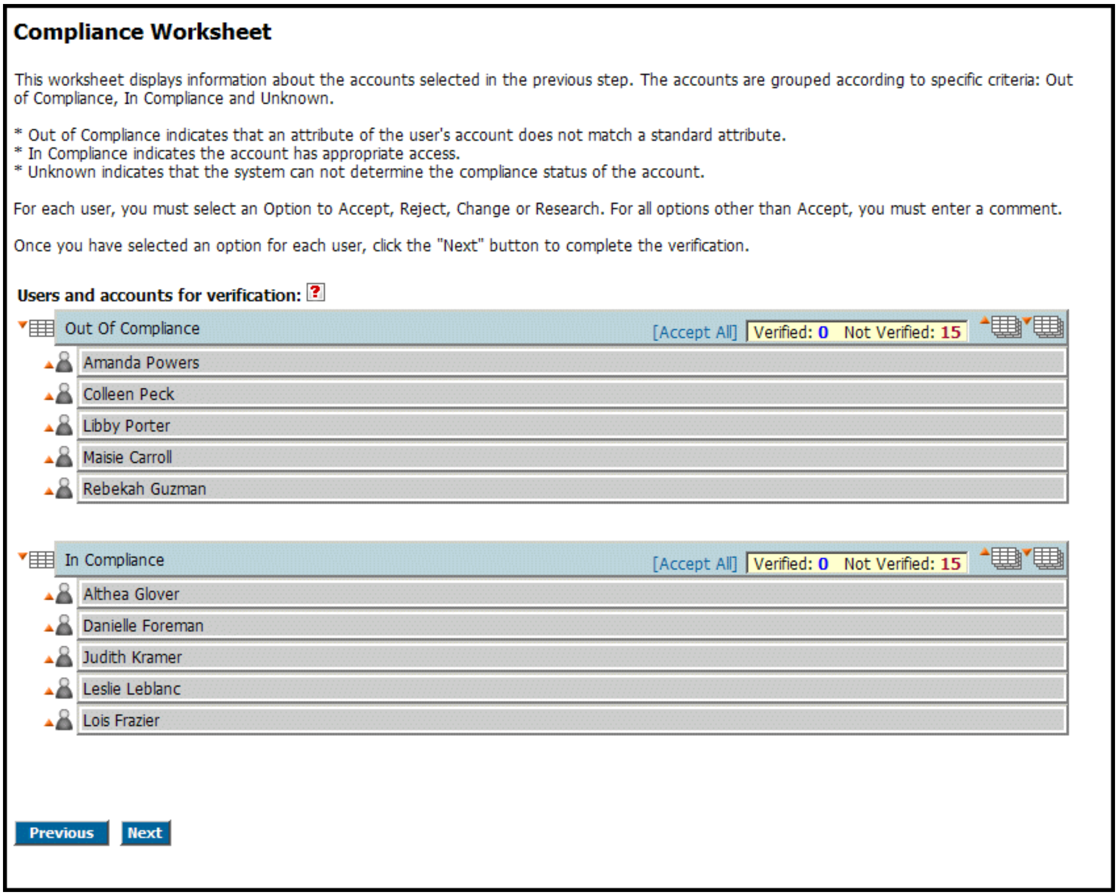
12. This workflow does not use worksheet rules, so you do not need to complete the **Worksheet Rule Configuration** section.

13. Click **SUBMIT**.

ComplianceCourier Worksheets

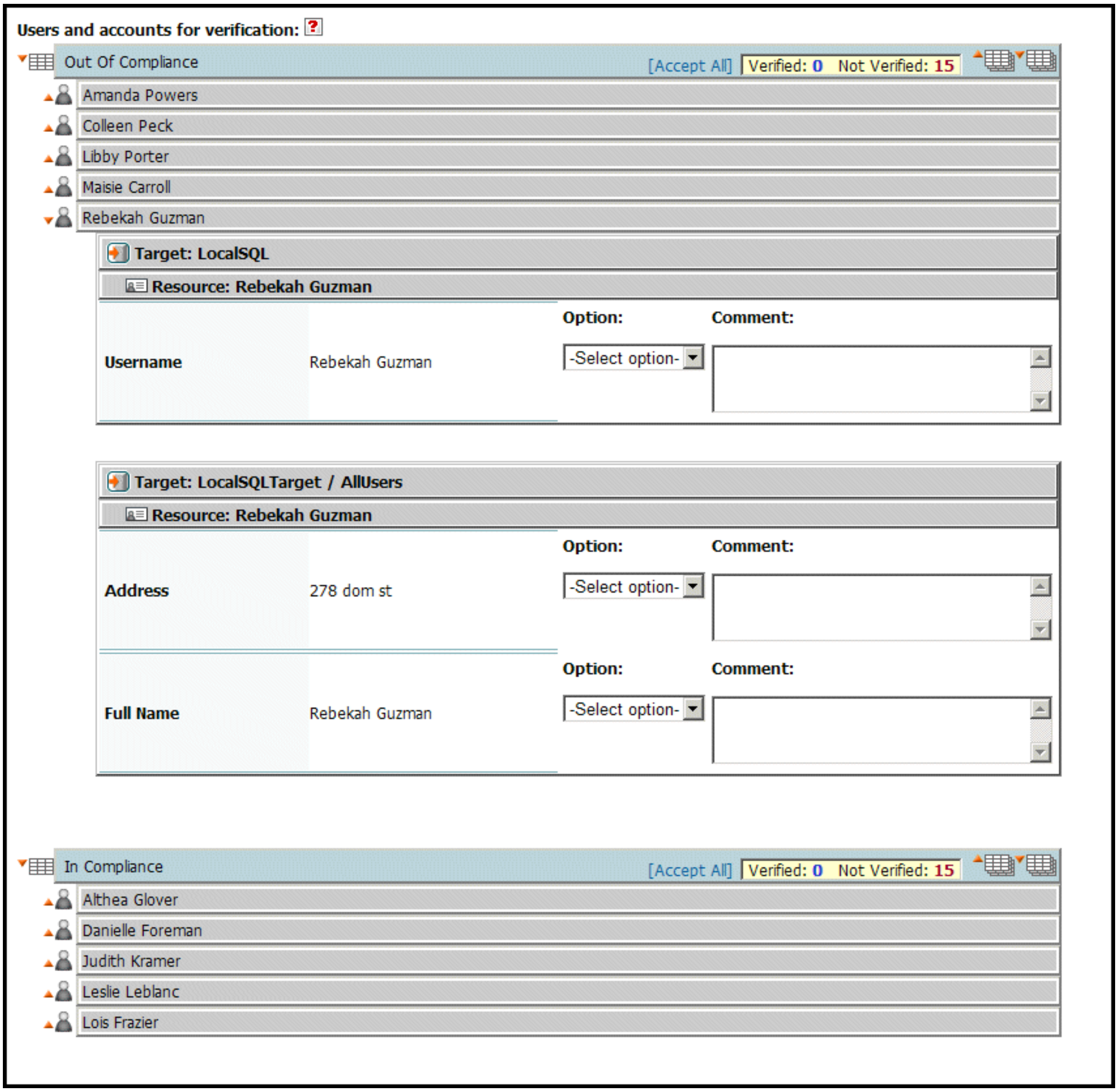
Figure 67 and *Figure 68* show examples of Compliance worksheets displayed to the provisioner.

Figure 67: Compliance Worksheet Screen



If you click on the icon of the person next to the user name, that user's record expands to show details of the user's account. The targets and attributes listed are the ones configured to **SHOW** on the Resource Data Selection Form (*Figure 61*). Clicking on the table icons with the up and down arrows will collapse or expand all user records for that particular sub-worksheet.

Figure 68: Compliance Worksheet Account Details



For each user, the provisioner must select a verification option. From the **OPTION:** pull down box, the provisioner can select how to verify an employee's compliance status: to accept it, to reject it, to change it, or to research the status further.

In the **COMMENT** box, the provisioner can enter text about the employee's compliance status. The Change and Research options require that the provisioner enter text to explain the reason for these selections. The provisioner must verify the status of each employee on the form before clicking **NEXT**.

As with the interactive worksheet, the standard worksheet includes the Table icons for expanding and collapsing the entire sub-worksheet and the **ACCEPT ALL** button to accept all users in a sub-worksheet.

Chapter 8: Configuring a Role Creation Workflow

This chapter describes how to configure a workflow to create roles and template accounts associated with those roles, using the Courion Role Creation sample workflow as a model.

A role is a representation of a set of access rights to resources and data that correspond to a business function. RoleCourier workflows utilize the same actions as AccountCourier workflows, but use different configuration settings. Instead of provisioning accounts belonging to individuals, RoleCourier workflows provision the roles themselves, along with template accounts associated with those roles. Once created, roles can then be used in AccountCourier and ComplianceCourier workflows, enabling the end user to provision accounts using the role as a model instead of an individual user.

The sections in this chapter use the Courion Role Creation sample workflow, providing practical examples of how to configure RoleCourier workflows:

- *"Details on Global Settings Specific to the Role Creation Workflow" on page 146* describes information specific to this workflow.
- *"Creating a Role" on page 148* describes using the Courion Role Creation sample workflow to create a new role and associated template accounts by mining existing user's accounts.
- *"Adding to an Existing Role" on page 173* describes using the Courion Role Creation sample workflow to create additional template accounts and add them to the role definition.

Details on Global Settings Specific to the Role Creation Workflow

When the sample workflows are installed during Express Configuration, a number of forms are pre-configured that are not described in this manual. You can modify these forms based on your specific needs. An overview of these forms, applying to all the sample workflows, is described in *"Global Settings" on page 13*.

Additionally, the following information is specific to the Courion Role Creation workflow:

Transaction Repository

The Role Creation workflow uses the transaction repository to store information about the role. It also contains the IdentityMap information. It uses the Connector for Microsoft ADO. For details, see *Table 5 on page 245*.

The Courion Role Connector takes data that is persisted with every provisioning transaction (Request), and adds definitional information to indicate to the system that this data is now a role definition, as opposed to the record of a request. It stores the persisted data in the transaction repository.

To the transaction repository, a role is an entity that consists of a collection of targets. Each target can have a collection of accounts, and each account can have a collection of attribute/value pairs. This data is collected whenever a Request is submitted to the transaction repository. If the Courion Role Connector is one of the targets in a provisioning action, it undertakes the necessary back-end data transformations to convert a normal request into a role definition. All data exposed on all targets (whether hidden or visible), becomes part of the role definition.

For details on the schema available to define roles, see the appendix "Transaction Repository Database Views" in the manual *"Configuring Workflows with the Enterprise Provisioning Suite Administration Manager"*:

Macros

The Role Creation workflow uses custom macros which substitute information gathered dynamically by the Courion Server into forms and messages displayed to the end user. Some of the custom macros were created for the Add action, to retrieve role information about the role to which accounts are being added.

These macros all begin with `RoleInfo:`*xxx*, where xxx is the attribute. For example, `RoleInfo:DepartmentName` returns the department assigned to the role.

Triggers

In the Role Creation workflow, there are several triggers already configured:

- **CreateUBT** creates an entry in the IdentityMap so the Role Repository target is available on the Select Accounts to Define Role screen.

- **ProvUBTADCleanup**, **ProvUBTCleanup**, **ProvUBTExchangeCleanup**, **UBTCleanup**, and **UBTCleanupFail** all are used to delete entries from the IdentityMap at the completion of the workflow. The reason for the deletion is that the role information is stored in Role Repository and you want to prevent duplication of this information in the IdentityMap to avoid potential problems.

  The triggers that begin with “ProvUBT” delete the IdentityMap entries for the individual template accounts that are created. If you are going to add additional targets to the workflow, you will want to create a trigger for each template account being created that will delete the IdentityMap entry for that account. You can use **ProvUBTADCleanup** as a model for creating additional triggers.

Unused Forms in the Role Creation Workflow

The following forms are not used in this workflow: Seed Refine Search, Seed Community, Role Refine Search, Role Community, Approval Community, Delegation Community, Resource Claiming, Resource Suggestions, Conditions, Account ID Generation.

Creating a Role

This section describes how to configure the Create action, using the Courion Role Creation sample workflow.

With this workflow, a provisioner creates a role record that is stored in the transaction repository, plus one or more template accounts on target systems that are associated with the role. The Role Creation workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Use the Mining Community to select a group of users whose account access most closely matches the role being created.
3. Select a single user to serve as the baseline for the role.
4. Select the individual attributes for each target associated with the role. For the attribute values, provisioners can view the values belonging to the members of the mining community, helping them to select appropriate values for the template accounts.

Note: To select the mining users and the baseline user, you need to claim accounts to populate the IdentityMap (if they have not been previously claimed). For details see *“Using the Self-Service Claiming Workflow” on page 25*. The CourionSelf-Service sample workflow is preconfigured to enable individual users to claim their own accounts.

The following sections describe configuration of the forms needed for the Create action:

- *“Configure Properties for the Create Action” on page 149* determines which forms are presented to the provisioner.
- *“Refine the List of Displayed Mining Profiles” on page 151* describes how to set up a form that the user can complete to filter the mining profiles available in the workflow’s community.
- *“Define a Mining Community” on page 152* describes how to set up a form that displays a table of users whose attributes can be “mined”. The mined attributes are then displayed, enabling a provisioner to model attributes based on a group of users in stead of a single user.
- *“Refine the List of Displayed Resource Profiles” on page 157* describes how to set up a form the provisioner can complete to filter the resource profiles available in the workflow’s community.
- *“Define a Resource Community” on page 159* describes how to set up a form that displays the user profiles available for modeling. The provisioner selects a profile and the provisioning application uses the unique identifier in the profile to search the IdentityMap for all the resources associated with the profile.
- *“Define the IdentityMap Screen Presentation for the Create Action” on page 163* describes how to set up a form that controls the appearance of the Select Accounts to Define Role form presented to the provisioner.
- *“Configure an Initial Profile” on page 165* describes how to set up a form the provisioner completes that specifies the fields required to create a basic profile record for the role.

- *"Specify Unique Resource Data Fields for the Target" on page 168* describes how to set up a form the provisioner completes that specifies the fields, and possible default values, required to create the new role.

The following instructions describe how to modify the settings in the Courion Role Creation workflow. If you have created a new workflow by copying Courion Role Creation, modify the forms in that workflow. See *"Copying Sample Workflows" on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the Create Action

To modify the Properties for Create Action Form:

Flowchart View

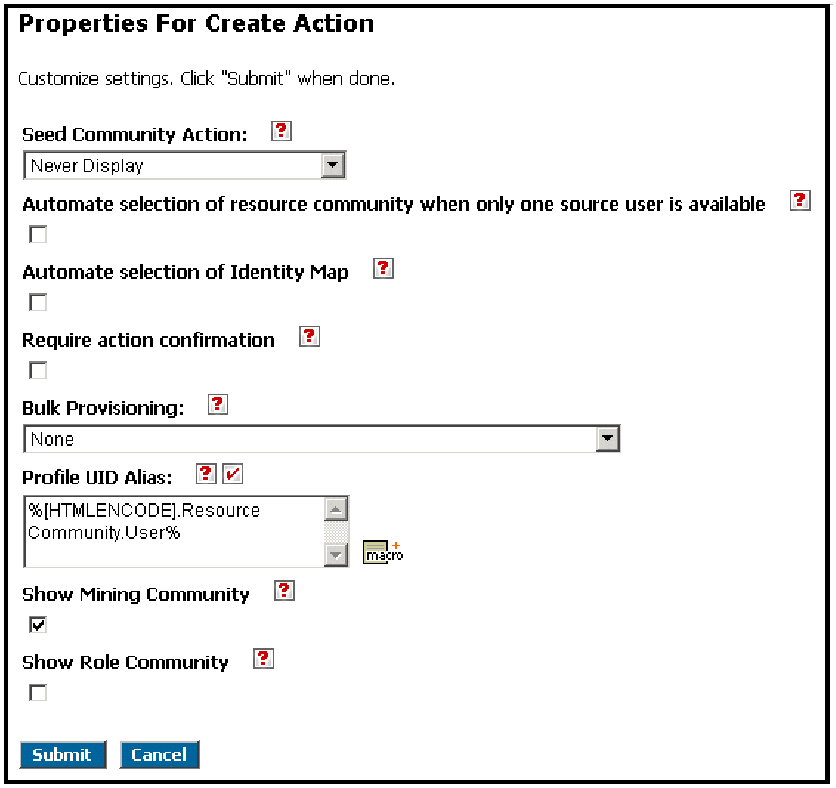
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Properties**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the  icon next to **Properties**.

   The Administration Manager displays the Properties for Create Action Form, shown in *Figure 69*.

Figure 69: Properties for Create Action Form



5. Leave the **Seed Community Action** option set to the default of Never Display. This workflow does not use the Seed Community.

6. Select the **Automate selection of resource community when only one source user is available** checkbox to enable automatic selection of the source profile (and bypass the Resource Community screen) when only a single source profile is retrieved from the connector. This setting is not selected by default.

   If you have created a special account as a baseline, check this checkbox. If you want the provisioner to be able to choose the baseline from a group of user accounts, leave the checkbox unchecked.

7. Select the **Automate selection of IdentityMap** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **Submit** button. This setting is turned off by default.

   In this workflow, the Resource Community is used to select a user as the baseline. Therefore, if this checkbox is selected, all of the baseline user's accounts are selected and therefore template accounts for the role are created on all those targets.

8. Select the **Require action confirmation** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.

9. Leave the **Bulk Provisioning** option set to the default of None. This workflow does not use Bulk Provisioning.

10. The **Profile UID Alias** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the Courion Role Creation sample workflow, this is set to%[HTMLENCODE].Resource Community.User%.
11. Leave the **Show Mining Community** checkbox selected since this workflow uses the mining community.
12. Leave the **Show Role Community** checkbox unselected since this workflow does not use the role community.
13. Click **Submit**.

Refine the List of Displayed Mining Profiles

The Courion Role Creation sample workflow uses the Mining Community to select a group of users whose account access most closely matches the role that is being created.

By default, RoleCourier displays all the users to the provisioner that meet the criteria configured in the Define Mining Community Form. If the filtering criteria for the Define Mining Community Form are broad or the company is large, the community of users can be extensive. You can select one or more fields to include on a Mining Refine Search Form. These fields are presented to the provisioner on the Search for Mining Community Candidates screen (*Figure 70*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of users that meet the Mining Refine Search criteria. The provisioner then selects one or more users from the list to be used for mining.

The provisioner can choose to skip entering data on the Search for Mining Community Candidates screen. If the screen is skipped, RoleCourier returns all the user profiles established by the Define Mining Community Form. You may also configure Mining Refine Search Form so that the Search for Mining Community Candidates screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Mining Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Mining Refine Search**.

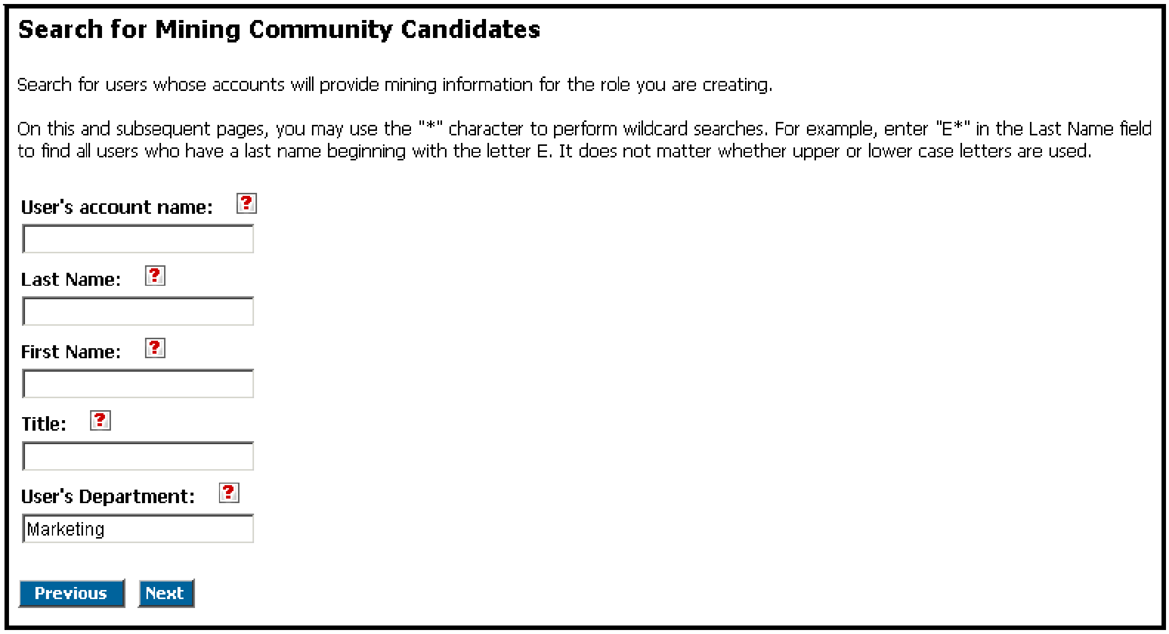
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the icon next to **Mining Refine Search**.

The process to refine the list of displayed profiles from a Mining Community in the Create action of the Role Creation workflow is the same as for a Create action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

Figure 70 shows the screen displayed to provisioner, based on the settings from the Role Creation workflow.

Figure 70: Refine Your Mining Community Search Screen



Define a Mining Community

The Mining Community is a set of existing users in a database or directory whose attributes may be used as a model for selecting attributes for an account that is being provisioned. In the case of role creation, the provisioner selects one or more users.

Note: The Mining Community is global and affects all actions within a workflow. Therefore, any changes made will apply to both the Create and Add actions in the Role Creation workflow.

Note: For the Mining Community to be displayed to the provisioner, you must select the **Show Mining Community** option on the Properties form. (This field is selected by default in the Role Creation workflow.)

Note: To use the Mining functionality, at least one attribute must have the **Mining** option selected in the **Presentation** field on the Unique Target Data Field Selection Form. See *"Specify Unique Resource Data Fields for the Target" on page 168* for details.

To modify the Define Mining Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.

4. Click on **Create Request**.
5. Click on **Mining Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

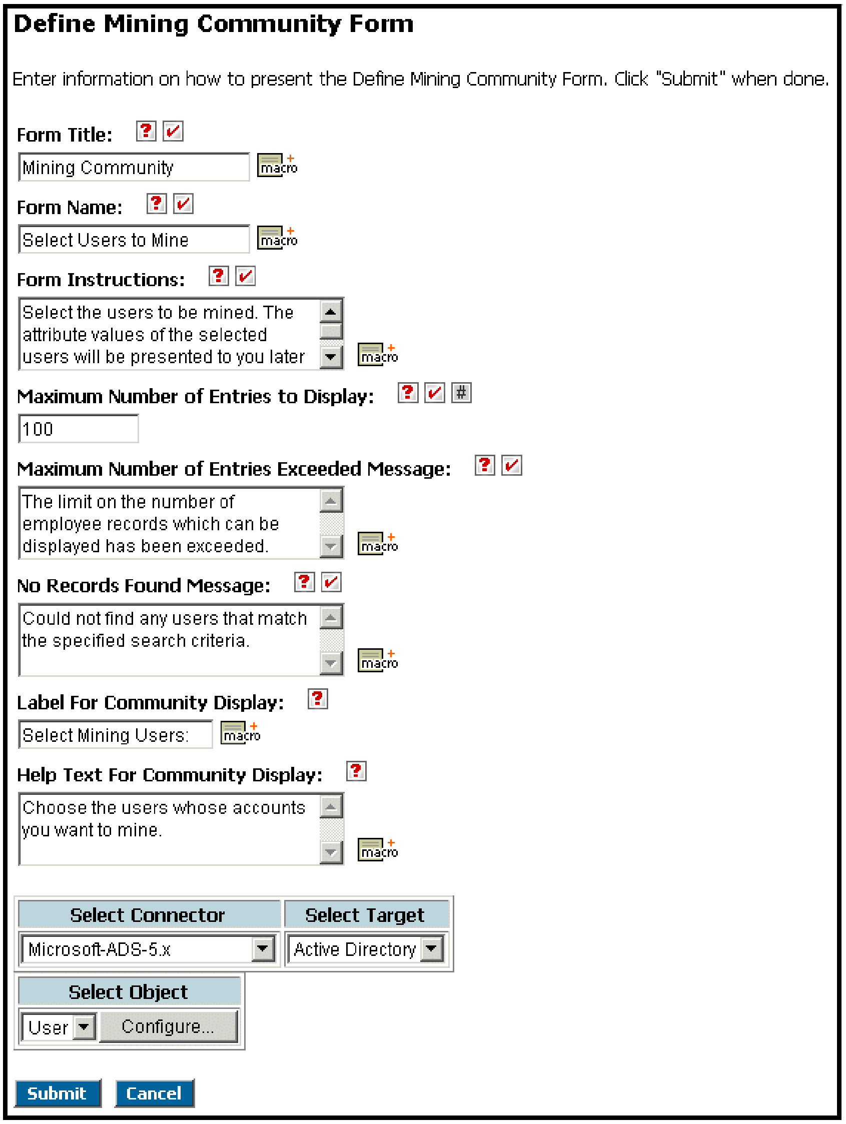
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Mining Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the  icon next to **Mining Community**.

   The Administration Manager displays the Define Mining Community Form, shown in *Figure 71* with default text and sample data. You can edit all text boxes.

Figure 71: Define Mining Community Form



5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.
7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Mining Refine Search Form, can help the provisioner limit the number of returned profiles (see *“Refine the List of Displayed Mining Profiles” on page 151*).
9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Mining Refine Search Form to display profiles that more closely match search criteria.

10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message will display if the provisioner has entered values on the Mining Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Mining Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label For Community Display** text box appears as a title over the Mining Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Select a connector from the **Select Connector** drop-down list box. In the sample workflow, this is the Connector for Microsoft Active Directory.

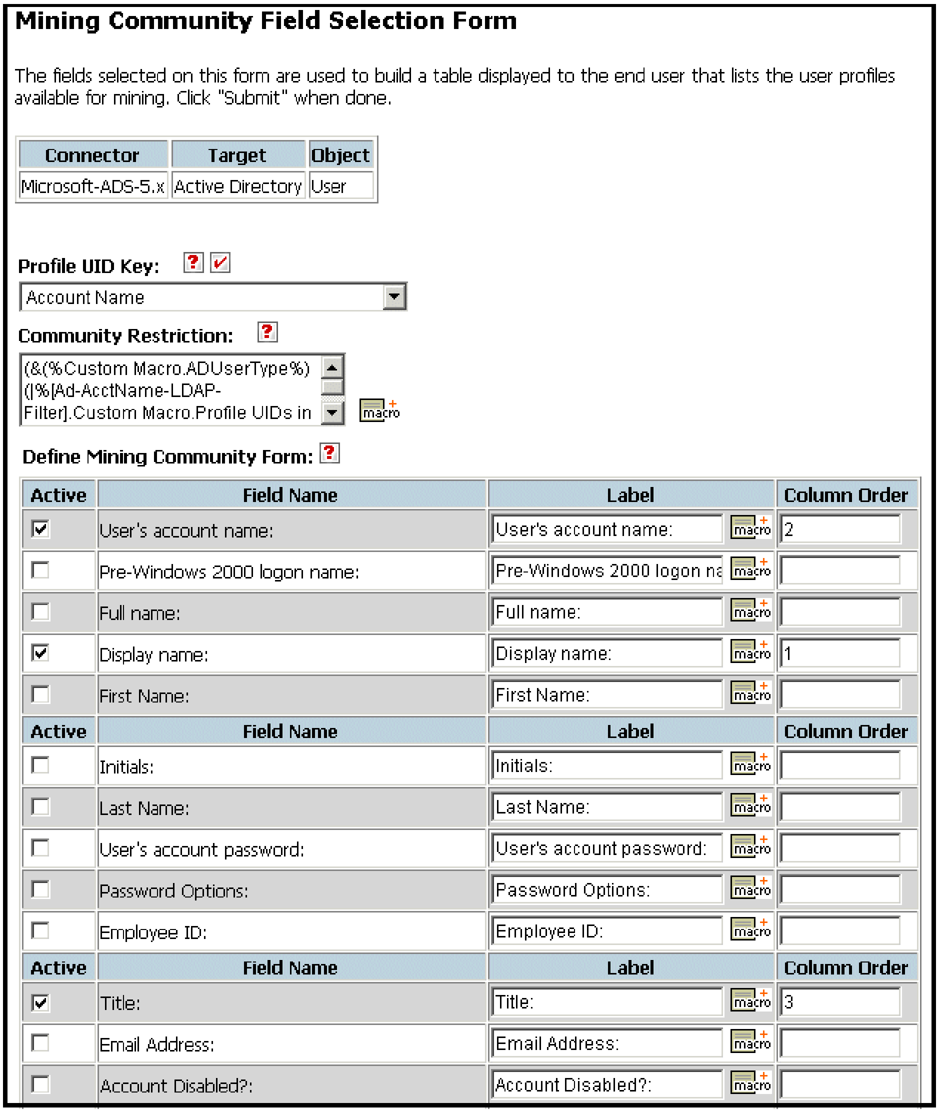
    Select a target from the **Select Target** drop-down list box.

    Select an object from the **Object** drop-down list box.
14. Click **Configure...**.

    The Administration Manager displays the Define Mining Community Field Selection Form, shown in *Figure 72*.

Note: The fields displayed on the form depend on the object selected. The list of fields has been shortened to save space.

Figure 72: Define Mining Community Field Selection Form



15. In the **PROFILE UID KEY** drop-down box, select the unique user ID field in this object that will serve as a link to a user's entries, identified by the Profile UID field, in the Resource Community table.

16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Statement syntax depends on the target datasource. Do not use hashed or encrypted fields in the statement.

    In the Role Creation workflow, the macro restricts return of available profiles to Active Directory records that belong to users, and only those users with a profile stored in the IdentityMap.

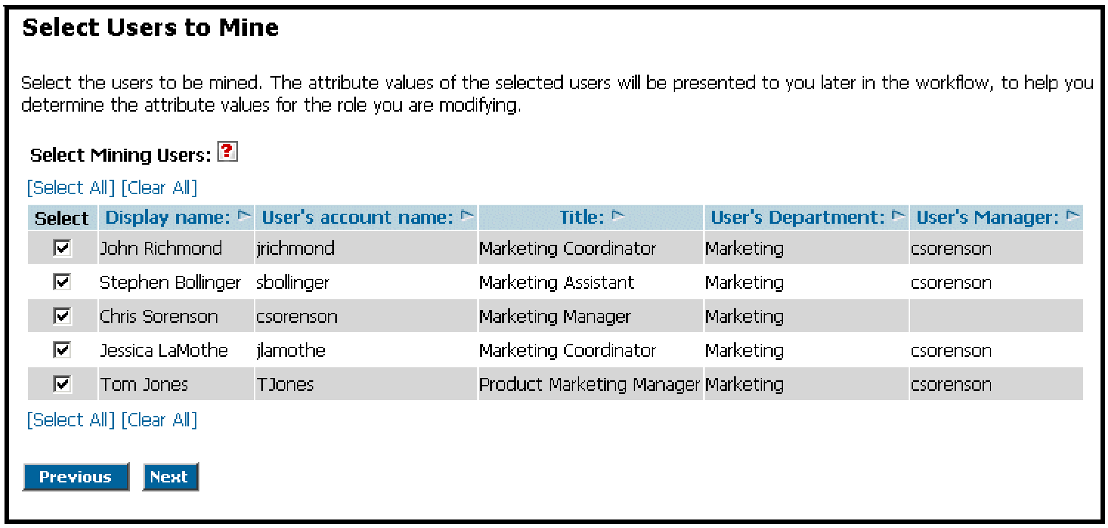
    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on Defining a Dynamic Community.

17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner.

18. The **Label** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change “EmployeeBadgeNumber” field to “Badge number:”.
19. In the **Column Order** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered “1” appears as the first column.
20. Click **Submit**.

Figure 73 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 73: Select Mining Users Screen



Select Users to Mine

Select the users to be mined. The attribute values of the selected users will be presented to you later in the workflow, to help you determine the attribute values for the role you are modifying.

Select Mining Users:

[Select All] [Clear All]

Select	Display name:	User's account name:	Title:	User's Department:	User's Manager:
☑	John Richmond	jrichmond	Marketing Coordinator	Marketing	csorenson
☑	Stephen Bollinger	sbollinger	Marketing Assistant	Marketing	csorenson
☑	Chris Sorenson	csorenson	Marketing Manager	Marketing	
☑	Jessica LaMothe	jlamothe	Marketing Coordinator	Marketing	csorenson
☑	Tom Jones	TJones	Product Marketing Manager	Marketing	csorenson

[Select All] [Clear All]

Previous Next

Refine the List of Displayed Resource Profiles

The Courion Role Creation sample workflow uses the Resource Community to select a baseline user account as a model for creating the role.

By default, RoleCourier displays all the users to the provisioner that meet the criteria configured in the Define Resource Community Form. If the filtering criteria for the Define Resource Community Form are broad or the company is large, the community of users could be extensive. You can select one or more fields to include on a Resource Refine Search Form. These fields are presented to the provisioner on the Search for Role Baseline Candidates screen (*Figure 74*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of users that meet the Resource Refine Search criteria. The provisioner then selects a user from the list as a model.

The provisioner can choose to skip entering data on the Search for Role Baseline Candidates screen. If the screen is skipped, RoleCourier returns all the user profiles established by the Define Resource Community Form. You may also configure Resource Refine Search Form so that the Search for Role Baseline Candidates screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Resource Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Resource Refine Search**.

Tree View

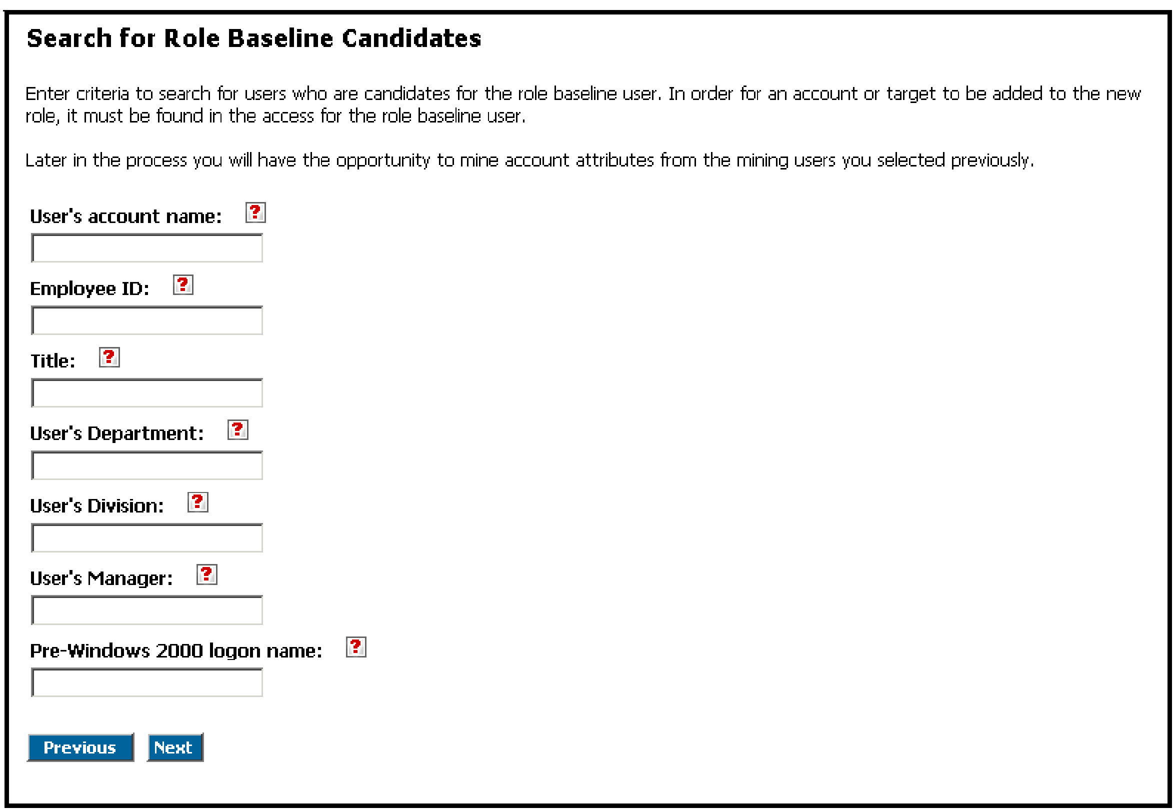
1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the icon next to **Resource Refine Search**.

The process to refine the list of displayed profiles from a Resource Community in the Create action of the Role Creation workflow is the same as for a Create action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Figure 74 shows the screen displayed to provisioner, based on the settings from the Role Creation workflow.

Figure 74: Search for Role Baseline Candidates Screen



Search for Role Baseline Candidates

Enter criteria to search for users who are candidates for the role baseline user. In order for an account or target to be added to the new role, it must be found in the access for the role baseline user.

Later in the process you will have the opportunity to mine account attributes from the mining users you selected previously.

User's account name:

Employee ID:

Title:

User's Department:

User's Division:

User's Manager:

Pre-Windows 2000 logon name:

Previous Next

Define a Resource Community

The Courion Role Creation sample workflow uses the Resource Community to select a baseline user account as a model for creating the role. The workflow then creates a role record that is stored in the transaction repository, plus one or more template accounts on target systems that are associated with the role. It is important to choose a baseline user account that has all the target accounts that you want to associate with the role, since additional targets can not be added in the workflow. (You can, however, use the Add to an Existing Role workflow to add additional targets. See *"Adding to an Existing Role" on page 173* for details.)

By using the Community Restriction parameter, found on the Resource Community Field Selection Form, you can restrict the resources that the provisioner can access. For example, you can set up a list that includes only the members of the Marketing department and restrict the provisioner to only provisioning resources associated with those members of the Marketing department.

In practice, the Community Restriction parameter is often used to select a single baseline user. This ensures that all necessary targets are available for the role. In this case, you can select the **Automate selection of resource community when only one source user is available** checkbox on the Properties Form, to enable automatic selection of the source profile (and bypass both the Resource Community and resource Refine Search screens).

Note: The Resource Community is global and affects all actions within a workflow. Therefore, any changes made will apply to both the Create and Add actions in the Role Creation workflow.

To modify the Define Resource Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Resource Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

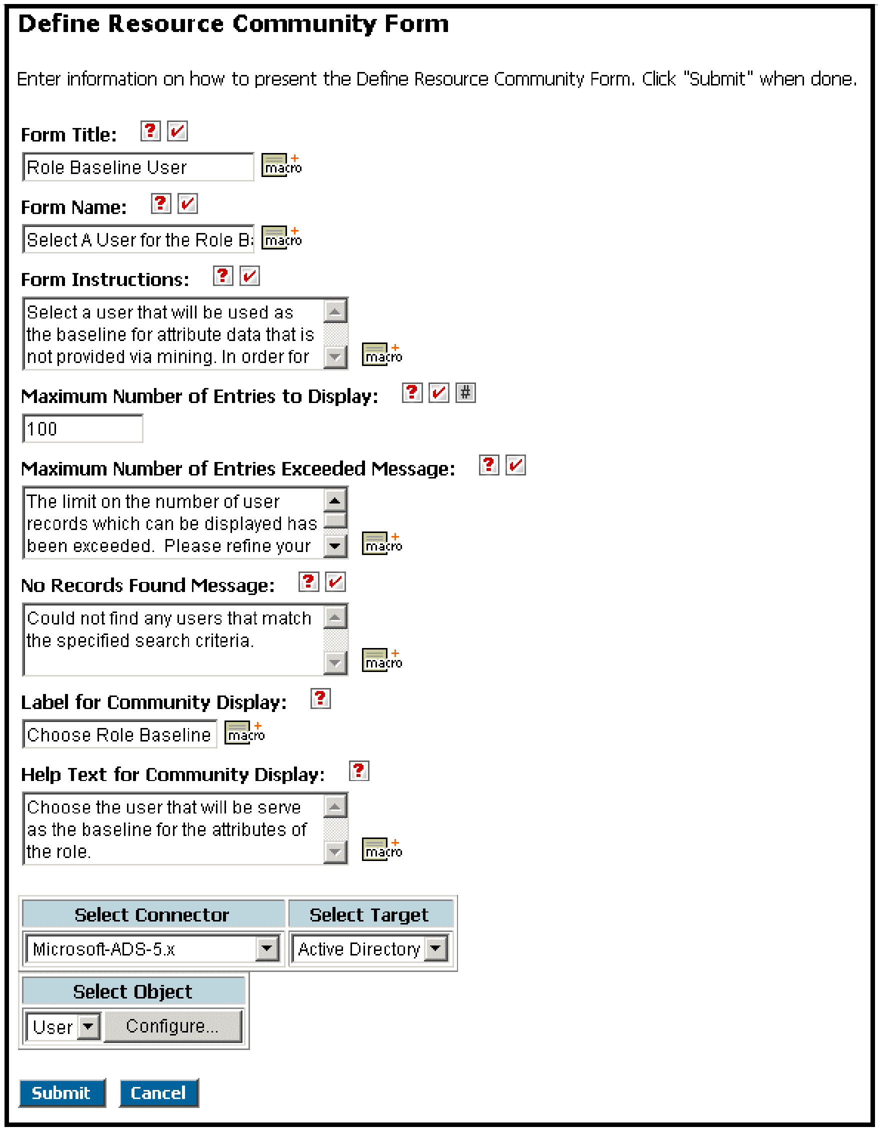
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Resource Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Resource Community**.

The Administration Manager displays the Define Resource Community Form, shown in *Figure 75* with default text and sample data. All text boxes can be edited.

Figure 75: Define Resource Community Form



5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.

6. Text in the **Form Name** text box appears as a title on the form.

7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the "<" and ">" is considered an HTML tag and is not displayed.)

8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Source Refine List Form, can help the provisioner limit the number of returned profiles (see *"Refine the List of Displayed Resource Profiles" on page 157*).

9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Source Refine Search Form to display profiles that more closely match search criteria.

10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message will display if the provisioner has entered values on the Source Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label for Community Display** text box appears as a title over the Resource Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Select a connector from the **Select Connector** drop-down list box. In the sample workflow, this is the Connector for Microsoft Active Directory.

    Select a target from the **Select Target** drop-down list box.

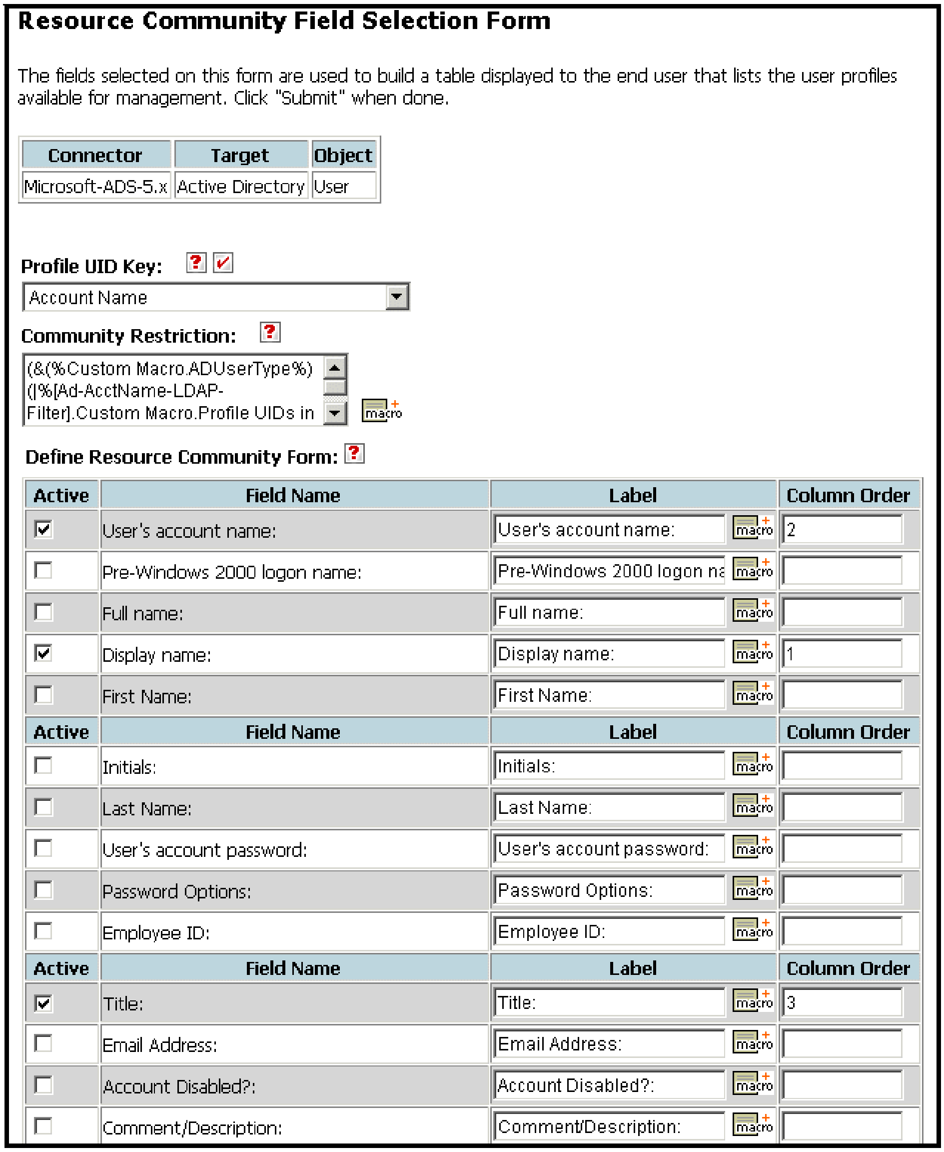
    Select an object from the **Object** drop-down list box.

    Note: The available connectors and targets depend on what has been provided through the Connector Configuration Manager. Collectively, the connector, target, and object point to the datasource that contains the user profiles available in this workflow.
14. Click **Configure...**.

    The Administration Manager displays the Resource Community Field Selection Form, shown in *Figure 76*.

    Note: The fields displayed on the form depend on the object selected. The list of fields has been shortened to save space.

Figure 76: Resource Community Field Selection Form



Resource Community Field Selection Form

The fields selected on this form are used to build a table displayed to the end user that lists the user profiles available for management. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADS-5.x	Active Directory	User

Profile UID Key:

Account Name

Community Restriction:

(&(%Custom Macro.ADUserType%)(|%[Ad-AcctName-LDAP-Filter].Custom Macro.Profile UIDs in

Define Resource Community Form:

Active	Field Name	Label	Column Order
☑	User's account name:	User's account name:	2
☐	Pre-Windows 2000 logon name:	Pre-Windows 2000 logon na	
☐	Full name:	Full name:	
☑	Display name:	Display name:	1
☐	First Name:	First Name:	
☐	Initials:	Initials:	
☐	Last Name:	Last Name:	
☐	User's account password:	User's account password:	
☐	Password Options:	Password Options:	
☐	Employee ID:	Employee ID:	
☑	Title:	Title:	3
☐	Email Address:	Email Address:	
☐	Account Disabled?:	Account Disabled?:	
☐	Comment/Description:	Comment/Description:	

15. In the **PROFILE UID KEY** drop-down box, select the unique user ID field in this object that will serve as a link to a user's entries, identified by the Profile UID field, in the Resource Community table.

16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Do not use hashed or encrypted fields in the statement.

    In the Role Creation workflow, the macro restricts return of available profiles to Active Directory records that belong to users, and only those users with a profile stored in the IdentityMap.

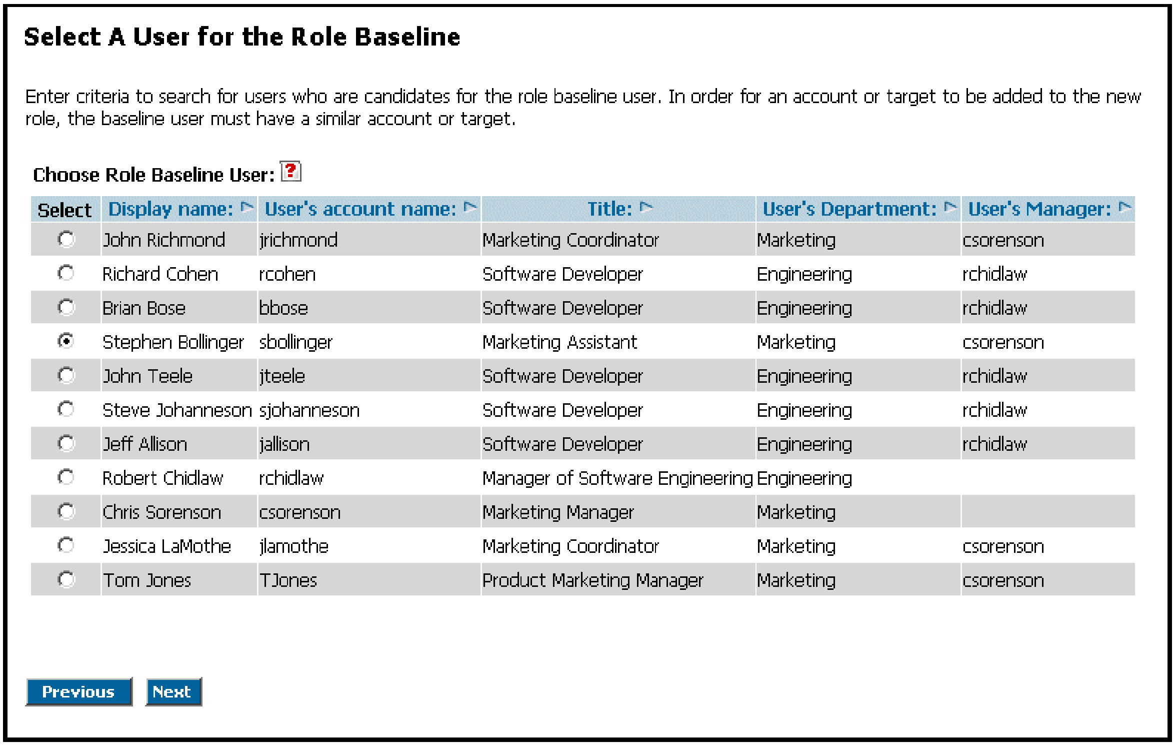
    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on this information.

17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change "EmployeeBadgeNumber" field to "Badge number:".

18. In the **Column Order** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered “1” appears as the first column.
19. Click **Submit**.

Figure 77 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 77: Select a User for the Role Baseline Screen



Select A User for the Role Baseline

Enter criteria to search for users who are candidates for the role baseline user. In order for an account or target to be added to the new role, the baseline user must have a similar account or target.

Choose Role Baseline User:

Select	Display name:	User's account name:	Title:	User's Department:	User's Manager:
○	John Richmond	jrichmond	Marketing Coordinator	Marketing	csorenson
○	Richard Cohen	rcohen	Software Developer	Engineering	rchidlaw
○	Brian Bose	bbose	Software Developer	Engineering	rchidlaw
◉	Stephen Bollinger	sbollinger	Marketing Assistant	Marketing	csorenson
○	John Teele	jteele	Software Developer	Engineering	rchidlaw
○	Steve Johanneson	sjohanneson	Software Developer	Engineering	rchidlaw
○	Jeff Allison	jallison	Software Developer	Engineering	rchidlaw
○	Robert Chidlaw	rchidlaw	Manager of Software Engineering	Engineering	
○	Chris Sorenson	csorenson	Marketing Manager	Marketing	
○	Jessica LaMothe	jlamothe	Marketing Coordinator	Marketing	csorenson
○	Tom Jones	TJones	Product Marketing Manager	Marketing	csorenson

Previous Next

Define the IdentityMap Screen Presentation for the Create Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Define Role screen, shown in *Figure 78*.

Note: If the **Automate selection of IdentityMap** on the Properties form is enabled, this form is skipped in the workflow, all of the baseline user’s accounts are selected, and the workflow proceeds to Unique Resource Data form (used to display the Enter Role Information screen to the provisioner).

To modify the IdentityMap Screen Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **IdentityMap Screen**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE CREATION** workflow.
3. Expand **ACTIONS** and expand **CREATE**.
4. Click the icon next to **IDENTITYMAP SCREEN**.

The process to modify the fields for the IdentityMap Screen in the Create action of the Role Creation workflow is the same as for a Create action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

For the Select Accounts to Define Role Screen, in the Courion Role Creation sample workflow you will see two tabs, labelled “Corporate Systems” and “Role Management”. The labels for these tabs are determined by the values chosen in the **CATEGORY** field found on the Add and Modify Target forms. Targets configured with the same category name will show up under a single tab. If no category is specified, the target will show up under a tab labelled “Accounts”. (For more details on configuring targets, refer to *Table 5 on page 245*.)

In the case of the sample workflow, the Courion Role Connector has been given its own separate category to help distinguish that this target is used for creation of the role itself, whereas the other targets are used to create template accounts that link to the role.

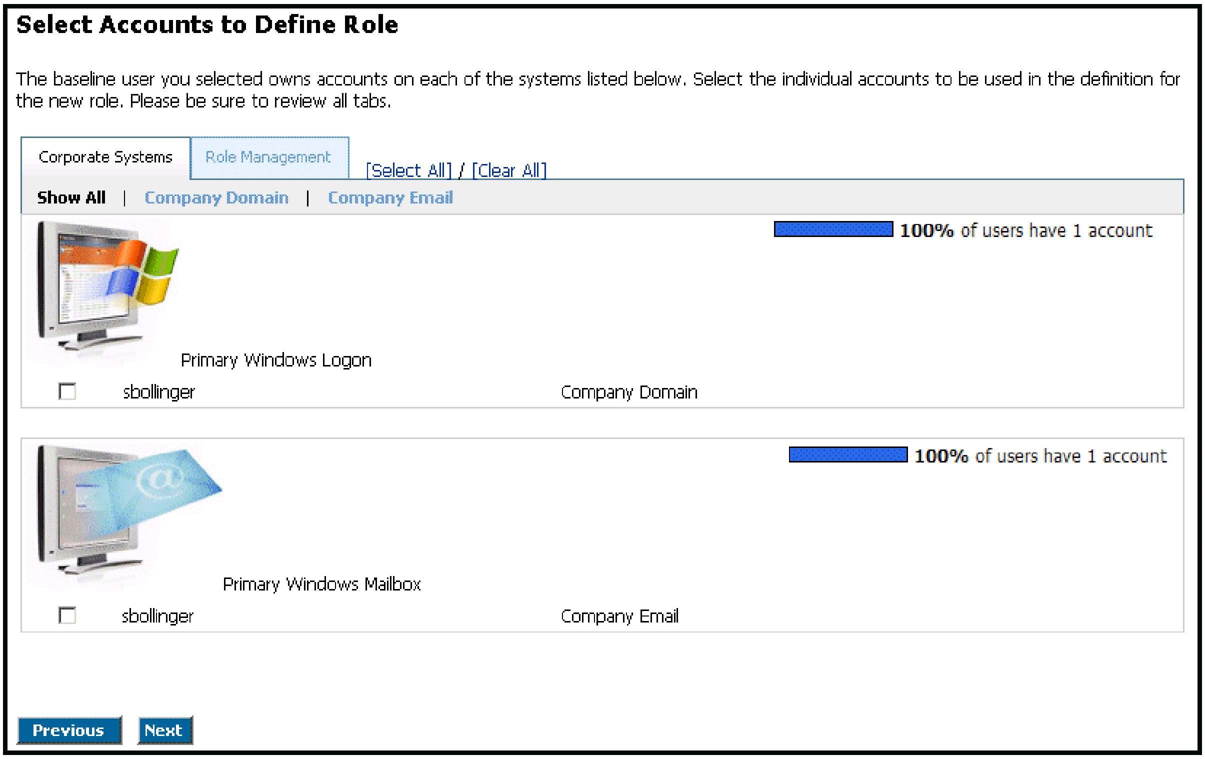
The names of the individual targets in the grey menu bar are taken from the **ALIAS** field on the Add and Modify Target forms. If no alias is specified, the **IDENTITYMAP TARGET ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. If one or more users have been selected from the mining community, both a resource description and a popularity indicator are displayed above the resource name, checkbox, and target name. The description is taken from the **DESCRIPTION** field on the Add and Modify Target forms. If no mining users are selected, only the resource name, checkbox, and target name are displayed. As shown in *Figure 78*, the description can include a graphic.

In addition to the Role Management target, the targets that are displayed are determined by the accounts owned by the user selected as the baseline. (The targets must also be configured on the Target Configuration Form.) For each target listed under a tab, the provisioner must select the target by checking the checkbox, if they want to create a template account for that target.

In the Role Creation workflow, the Role Management target is selected automatically and may not be unselected. (If not selected, the role would not be created.) This is determined by the RoleSampleIDMap.xslt file assigned in the **XSLT FILE FOR PROCESSING** field.

Figure 78: Select Accounts to Define Role Screen



Configure an Initial Profile

In the Courion Role Creation sample workflow, the Initial Profile form is used to collect basic data about the role that is used when the role and associated template accounts are created. No actual profile is created, since that does not apply to the creation of a role.

To modify the Initial Profile Form:

Flowchart View

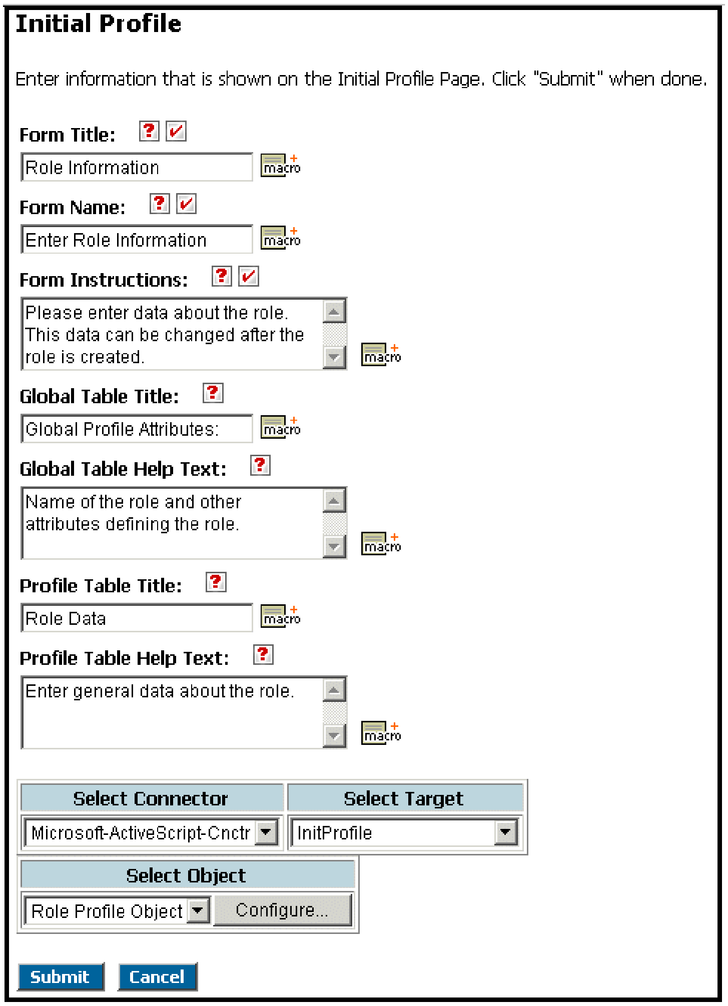
1. Log in to the Administration Manager Flowchart View.
2. Select **COURION ROLE CREATION** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CREATE** from the **ACTION** drop-down menu.
4. Click on **CREATE REQUEST**.
5. Click on **INITIAL PROFILE**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE CREATION** workflow.
3. Expand **ACTIONS** and expand **CREATE**.
4. Click the icon next to **INITIAL PROFILE**.

   The Administration Manager displays the Initial Profile Form, shown in *Figure 79* with default text and sample data. All text boxes can be edited.

Figure 79: Initial Profile Form



5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.

6. Text in the **Form Name** text box appears as a title on the form.

7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the "<" and ">" is considered an HTML tag and is not displayed.)

8. Text in the **Global Table Title** text box appears as the title on Global Fields Table.

9. Text in the **Global Table Help Text** box appears as the help text in the Global Fields Table.

10. Text in the **Profile Table Title** text box appears as the title for each user's profile table.

11. Text in the **Profile Table Help Text** box appears as the help text in the Profile Table.

12. The **Select Connector**, **Select Target**, and **Select Object** fields are set to use a specific script for Microsoft Active Script, which prevents creation of a profile and passes the information collected here to the targets.

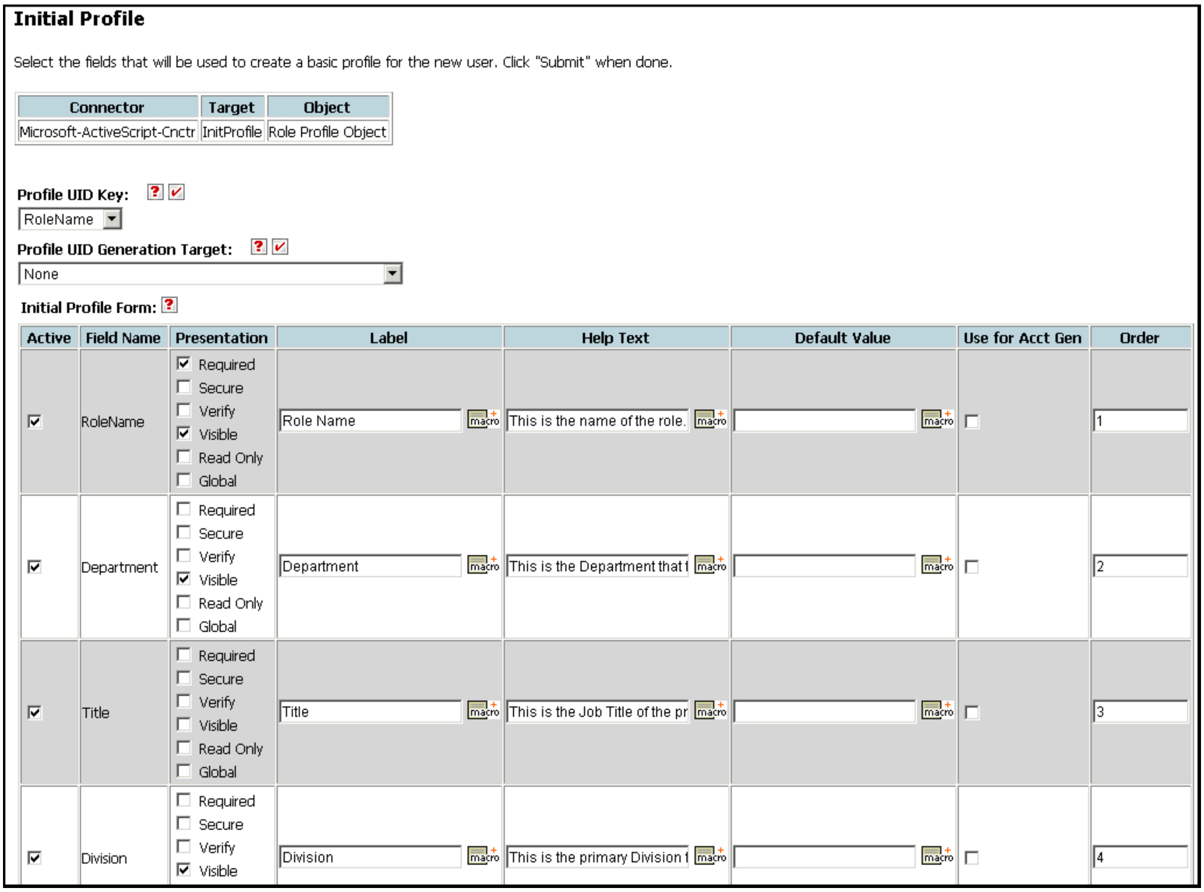
13. Click **Configure...**.

The Administration Manager displays the Initial Profile Select Fields Form, shown in *Figure 80*.

Note: The fields displayed depend on the object selected. The list of fields has been shortened to save space. *Figure 80* shows sample selections.

Note: When creating an initial profile in Sun Directory Server, do not use the aci attribute. This attribute exceeds the maximum length for the field, causing the creation to fail.

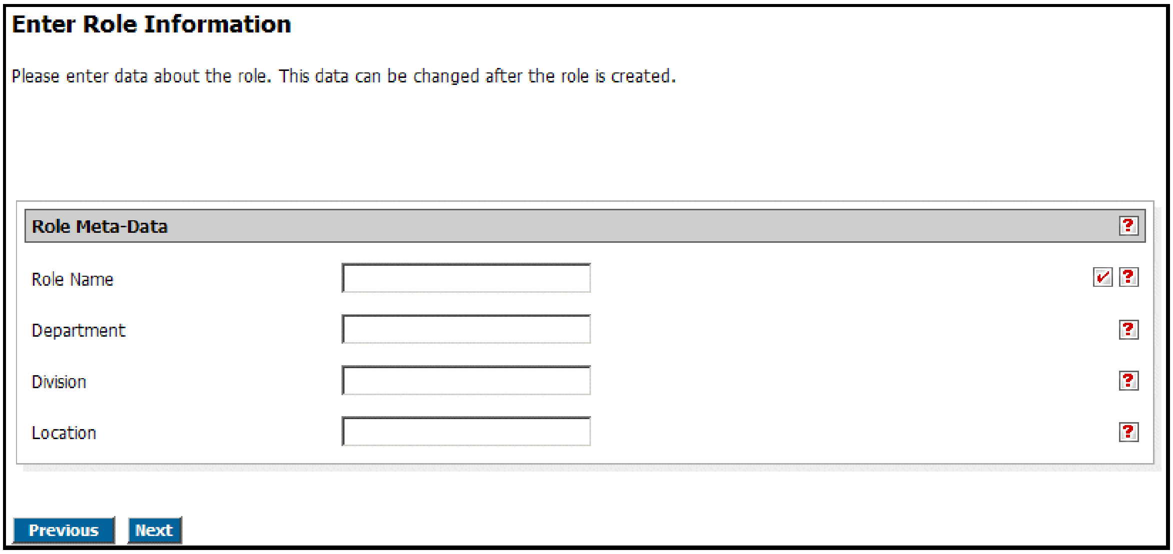
Figure 80: Initial Profile Select Fields Form



14. Select the fields to include in the initial profile for a new user. For a description of all fields, refer to *Table 2 on page 71*.
15. The **Profile UID Key** drop-down box lists all configured targets for resource creation.
16. The **Profile UID Generation Target** drop-down box lists the targets whose generated resource names may be used as the Profile UID key.
17. Click **Submit**.

Figure 81 shows an example of the Initial Profile form that the provisioner sees.

Figure 81: Enter Role Information Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are used to provision the template accounts that are linked to the role. The Unique Target Data form displays the currently available targets for which template accounts can be created. The Courion Role Creation sample workflow has three targets already configured—the Role Repository (for creation of the role itself), Active Directory (for a logon ID), and Microsoft Exchange (for an email account). If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. Refer to *Table 5 on page 245* for information on this form.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which will display mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

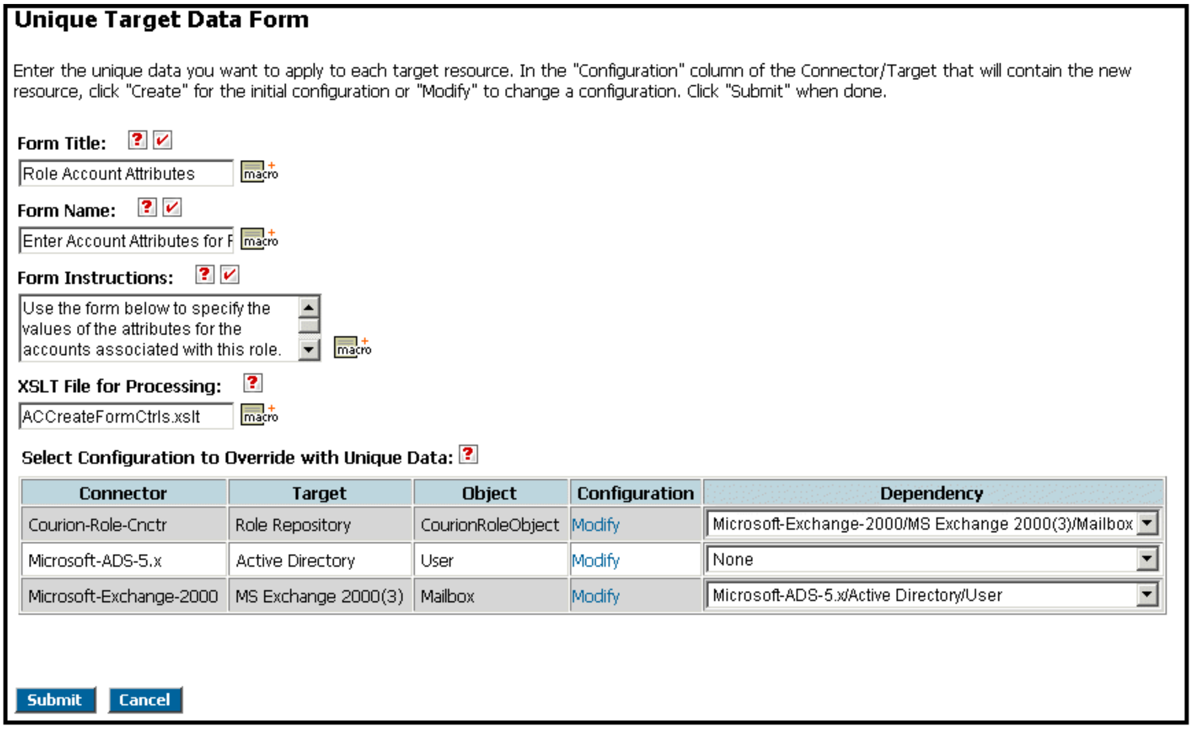
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the icon next to **Unique Resource Data**.

The Administration Manager displays the Unique Target Data Form, shown in *Figure 82* with default text and sample data. All text boxes can be edited. Data fields depend on the available connectors and targets.

Figure 82: Unique Target Data Form



5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.

6. Text in the **Form Name** text box appears as a title on the form.

7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)

8. Specify the file name or a macro that selects the **XSLT File for Processing**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTLML controls are rendered, controlling how provisioners interact with the data.

   To customize an XSLT file, copy the default file provided by Core Security and rename it. Then edit the renamed file as needed and assign that file to this field.

9. In the **Dependency** column, select the name of the target where the first resource must be successfully provisioned before any other resources are provisioned.

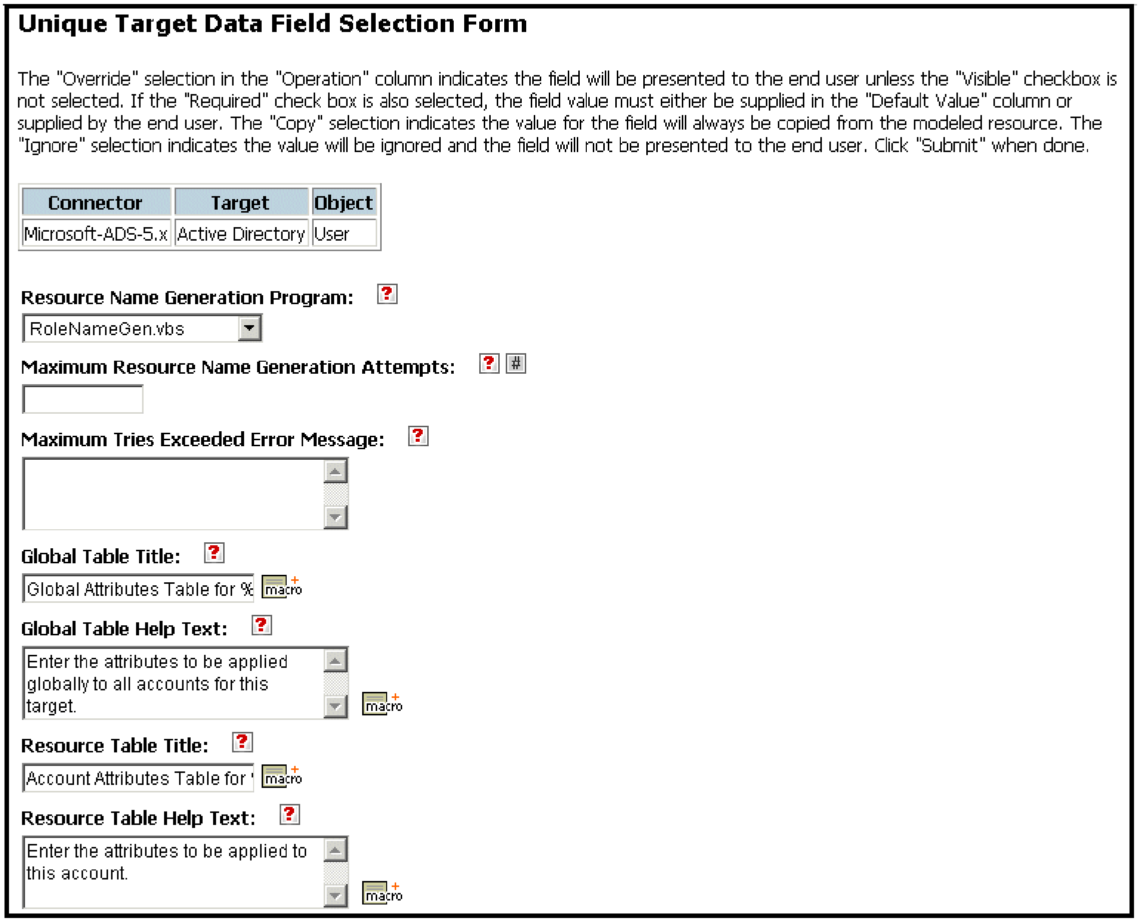
   Note: In the Role Creation sample workflow, the dependencies are configured serially, so the role record will not be created if any of the other accounts are unable to be provisioned. If you add any additional targets, Core Security recommends that you maintain this configuration by chaining your new targets to be dependent on existing targets and then change the dependency of the Role Repository so that it is the final target in the chain.

10. In the **Configuration** column, click **Modify** to change the attribute settings for the Role Repository, Active Directory, or Exchange accounts. If you have added any additional targets, click **Create**.

The Administration Manager displays the Unique Target Data Field Selection Form (*Figure 83*).

The actual content of this form depends on the connector. *Figure 83* shows the top of the form for the Connector for Microsoft Active Directory.

Figure 83: Unique Target Data Field Selection Form



Unique Target Data Field Selection Form

The "Override" selection in the "Operation" column indicates the field will be presented to the end user unless the "Visible" checkbox is not selected. If the "Required" check box is also selected, the field value must either be supplied in the "Default Value" column or supplied by the end user. The "Copy" selection indicates the value for the field will always be copied from the modeled resource. The "Ignore" selection indicates the value will be ignored and the field will not be presented to the end user. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADS-5.x	Active Directory	User

Resource Name Generation Program: ?
RoleNameGen.vbs

Maximum Resource Name Generation Attempts: ? #

Maximum Tries Exceeded Error Message: ?

Global Table Title: ?
Global Attributes Table for %
macro

Global Table Help Text: ?
Enter the attributes to be applied globally to all accounts for this target.
macro

Resource Table Title: ?
Account Attributes Table for '
macro

Resource Table Help Text: ?
Enter the attributes to be applied to this account.
macro

11. RoleCourier can automatically generate a resource name on each selected target system.

    In the Role Creation workflow, for the Microsoft Active Directory and Microsoft Exchange 2000 connectors, the RoleNameGen.vbs script is used to generate account names based on the role name. If you are adding targets to the workflow, assign this script to **Resource Name Generation Program** and then assign the appropriate macro to the account name attribute for the target. For more info, see *Table 5 on page 245*.

12. Text in the **Global Table Title** text box appears as the heading for the Global Attributes table.

13. Text in the **Global Table Help Text** text box appears as the help for the Global Attributes table.

14. Text in the **Resource Table Title** text box appears as the heading for each Resource Attributes table.

15. Text in the **Resource Table Help Text** text box appears as the help for the Resource Attributes table.

16. Configure the attributes for the target. You can determine whether or not an attribute is exposed to the provisioner, whether it is required, whether the values may be mined from the Mining Community, etc. Up to twenty-five attributes for the selected target are displayed in a table. To view additional attributes, click the "next page" icon at the bottom of the table. For a description of all fields, see *Table 4 on page 77*.

    Some attributes allow for multiple values (in particular, the Group Membership attribute in Microsoft Active Directory). See *Table 5 on page 245* for more information.

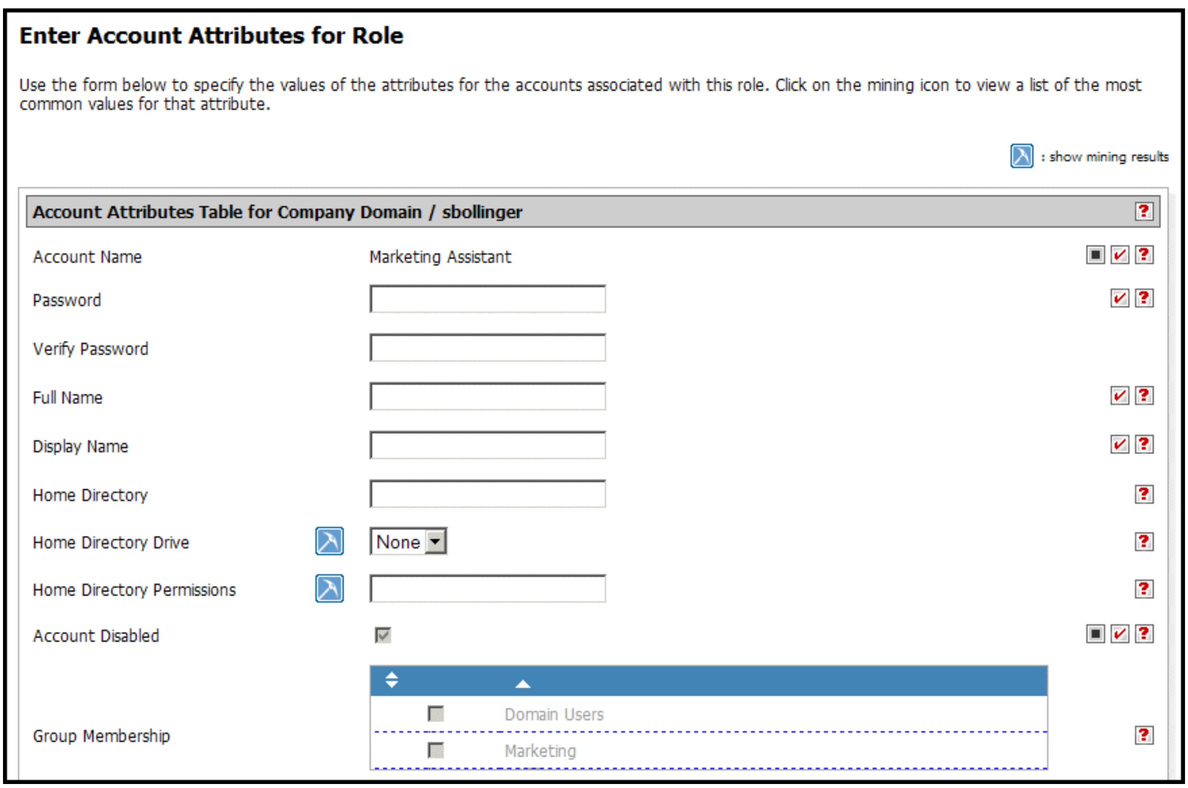
17. Click **SUBMIT** after completing the Unique Target Data Field Selection Form.

    The Administration Manager redisplays the Unique Target Data Form (*Figure 82*).

18. Click **CREATE** or **MODIFY** for another connector to configure the set of attributes for another resource or click **SUBMIT** to finish.

Figure 84 shows an example of part of the Enter Account Attributes screen displayed to the provisioner.

Figure 84: Enter Account Attributes for Role Screen

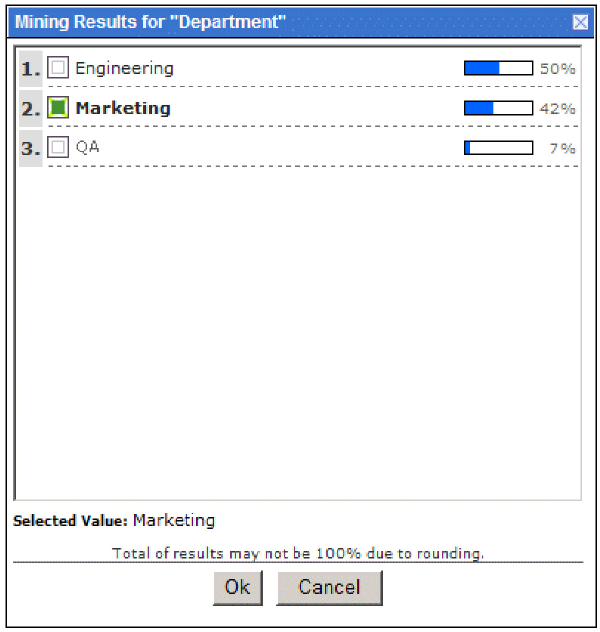


If the provisioner clicks on the Mining Icon, the Mining Results dialog box is displayed, as shown in *Figure 85*. (The Mining icon only appears if the **MINING** checkbox was selected in the **PRESENTATION** field on the Unique Target Data Field Selection Form.) The eight most common values for that attribute are displayed, along with the percentage of accounts within the Mining Community that contain the specific value. The value used by the baseline account is indicated by the green box.

Note: The percentage amounts of all the attribute values may not add up to 100%, due to the fact that percentage amounts are rounded down, and also because only the eight most common values are displayed.

Note: By default, the attribute values are case sensitive. So, for example, “Manager” will show up as a separate value from “manager”. If you want the attribute values to be case insensitive, change the **XSLT FILE FOR PROCESSING** field on the Unique Target Data Form from its default value of “ACCreateFormCtrls.xslt” to "CaseInsensitiveOverridesMining.xslt".

Figure 85: Mining Results



Adding to an Existing Role

This section describes how to configure the Add action using the Courion Role Creation sample workflow. This action enables a provisioner to add associated template accounts to existing roles.

With this workflow, a provisioner selects a role record that is stored in the transaction repository, and then creates template accounts that are associated with the role. The Role Creation workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing role.
3. Use the Mining Community to select a group of users whose account access most closely matches the selected role.
4. Select a single user to serve as the baseline for the role.
5. Select the additional targets to associate with the role, and then select the individual attributes for those targets. For the attribute values, provisioners can view the values used by members of the mining community, helping them to select appropriate values for the template accounts.

The following sections describe configuration of the forms needed for the Add action:

- *"Configure Properties for the Add Action" on page 174* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 176* describes how to set up a form the provisioner can complete to filter the role accounts available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 177* describes how to set up a form that displays the available role accounts. The provisioner selects the role for which they want to add template accounts.
- *"Refine the List of Displayed Mining Profiles" on page 182* describes how to set up a form the provisioner can complete to filter the profiles available in the workflow's mining community.
- *"Define a Mining Community" on page 183* describes how to set up a form that displays a table of users whose attributes can be "mined". The mined attributes are then displayed, enabling a provisioner to model attributes based on a group of users in stead of a single user.
- *"Refine the List of Displayed Resource Profiles" on page 184* describes how to set up a form the provisioner can complete to filter the profiles available in the workflow's resource community.
- *"Define a Resource Community" on page 184* describes how to set up a form that displays the provisionee profiles available for modeling. The provisioner selects a profile and the provisioning application uses the unique identifier in the profile to search the IdentityMap for all the resources associated with the profile.
- *"Define the IdentityMap Screen Presentation for the Add Action" on page 185* describes how to set up a form that controls the appearance of the Select Accounts to Add to Role form presented to the provisioner.

- *“Specify Unique Resource Data Fields for the Target” on page 187* describes how to set up a form the provisioner completes that specifies the fields, and possible default values, required to add the new resource.

Configure Properties for the Add Action

To modify the Properties for Add Action Form:

Flowchart View

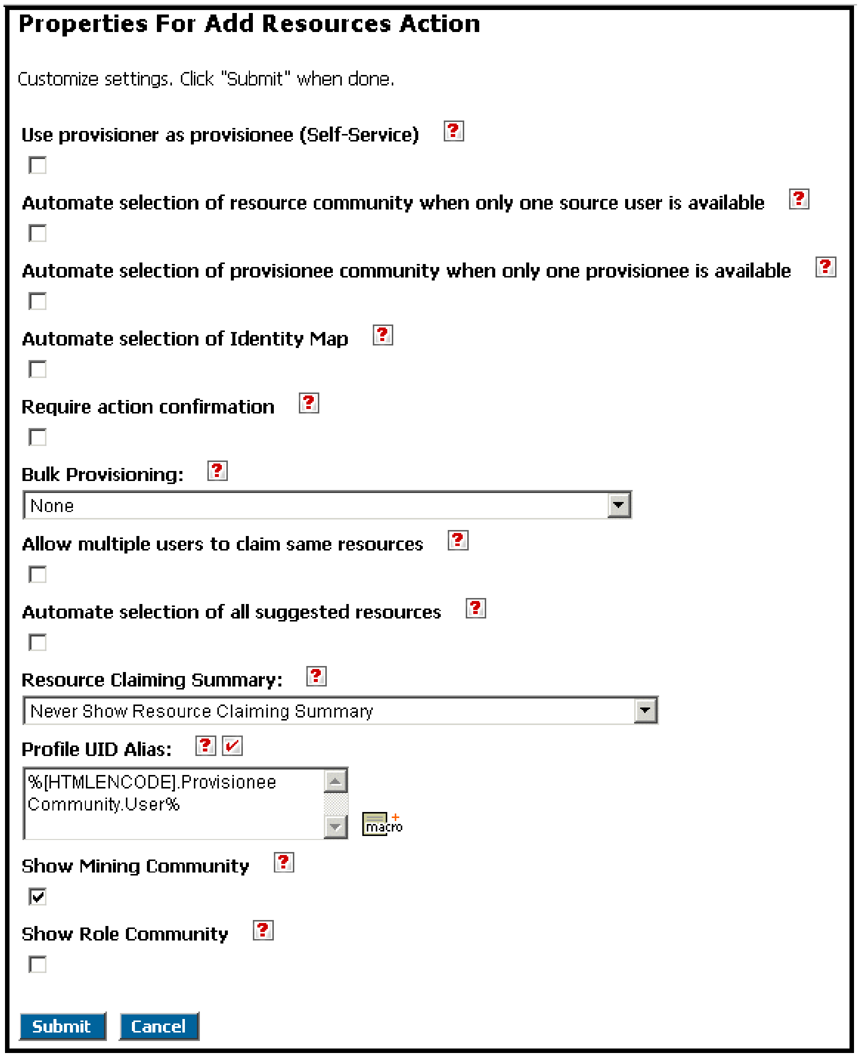
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Properties**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Properties**.

   The Administration Manager displays the Properties for Add Action Form, shown in *Figure 69*.

Figure 86: Properties for Add Action Form



5. Leave the **USE PROVISIONER AS PROVISIONEE (SELF-SERVICE)** checkbox unchecked, since it does not apply in this workflow.

6. Select the **AUTOMATE SELECTION OF RESOURCE COMMUNITY WHEN ONLY ONE SOURCE USER IS AVAILABLE** checkbox to enable automatic selection of the source profile (and bypass the Resource Community screen) when only a single source profile is retrieved from the connector. This setting is not selected by default.

   If you have created a special account as a baseline, check this checkbox. If you want the provisioner to be able to choose the baseline from a group of user accounts, leave the checkbox unchecked.

7. Select the **AUTOMATE SELECTION OF PROVISIONEE COMMUNITY WHEN ONLY ONE PROVISIONEE IS AVAILABLE** checkbox to enable automatic selection of the provisionee profile (and to bypass the Provisionee Community screen) when only a single provisionee profile is retrieved from the connector. This setting is not selected by default.

   Since the “provisionee” is the role itself in the Role Management workflow, if this field is selected, it would be necessary to authenticate into the workflow using the role’s account name and password. Therefore it is likely you would not want to select this field.

8. Select the **Automate selection of IdentityMap** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **Submit** button. This setting is turned off by default.

   In this workflow, the Resource Community is used to select a user as the baseline. Therefore, if this checkbox is selected, all of the baseline user's accounts are selected and template accounts for the role are created on all those targets. If a template account already exists on a target, a second one is created. For this reason, you leave this box unchecked.

9. Select the **Require action confirmation** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.

10. Leave the **Bulk Provisioning** option set to the default of None. This workflow does not use Bulk Provisioning.

11. Leave the **Allow multiple users to claim same resources** and **Automate selection of all suggested resources** checkboxes unchecked since this workflow does not use resource claiming.

12. Leave the **Resource Claiming Summary** option set to "Never show resource claiming summary" since this workflow does not use resource claiming.

13. The **Profile UID Alias** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the Courion Role Creation sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.

14. Leave the **Show Mining Community** checkbox selected since this workflow uses the mining community.

15. Leave the **Show Role Community** checkbox unselected since this workflow does not use the role community.

16. Click **Submit**.

Refine the List of Displayed Provisionee Profiles

In the Add action of the Role Creation workflow, the "provisionee" is the role itself.

By default, RoleCourier displays all the role records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of roles can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Role Search screen (*Figure 87*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of roles that meet the Provisionee Refine Search criteria. The provisioner then selects a role from the list in which accounts are added.

The provisioner can choose to skip entering data on the Role Search screen. If the screen is skipped, RoleCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Role Search screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the navigation bar.
4. Click on **Add Request** and click on **Provisionee Refine Search**.

Tree View

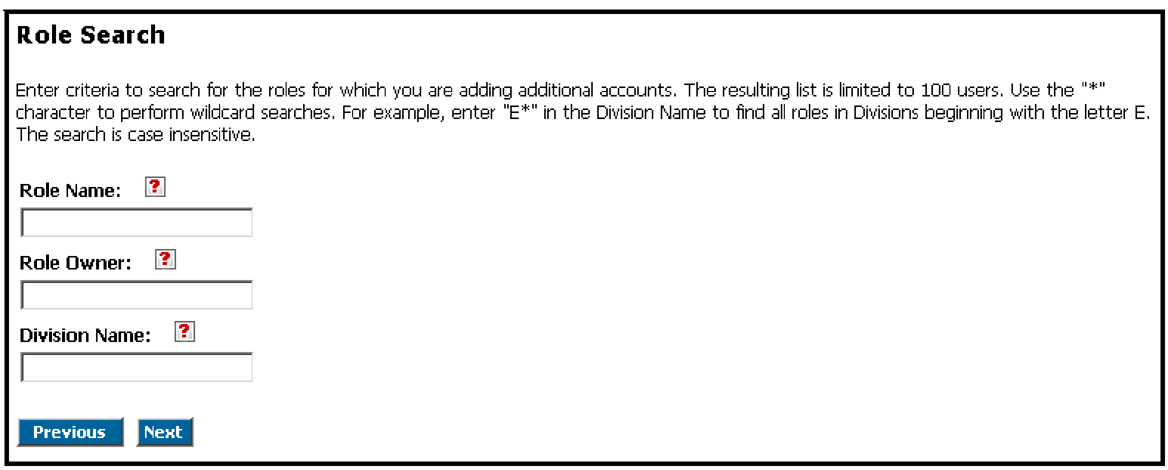
1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Provisionee Refine Search**.

The process to refine the list of displayed profiles from a Provisionee Community in the Add action of the Role Creation workflow is the same as for an Add action in any provisioning workflow. (The major difference is that instead of search for users, the provisioner is searching for roles. This is determined by the selection of the RoleCommunityView object in the transaction repository, which is configured on the Define Provisionee Community form.)

Refer to *Table 5 on page 245* for information on this form.

Figure 87 shows the screen displayed to provisioner, based on the settings from the Role Creation workflow.

Figure 87: Role Search



Define a Provisionee Community

In the Role Creation workflow, the “provisionee” is the role itself. The Provisionee Community consists of the role records stored in the transaction repository.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

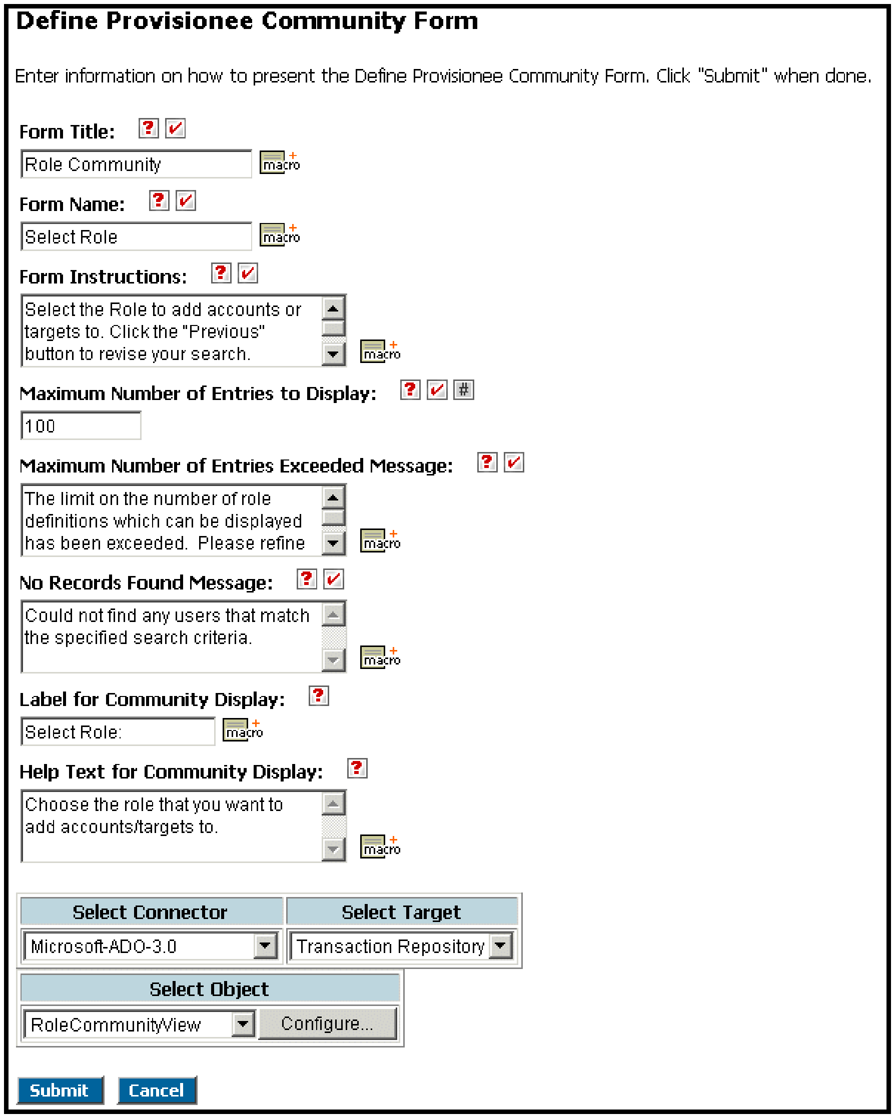
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Provisionee Community**.

   The Administration Manager displays the Define Provisionee Community Form, shown in *Figure 88* with default text and sample data. You can edit all text boxes.

Figure 88: Define Provisionee Community Form



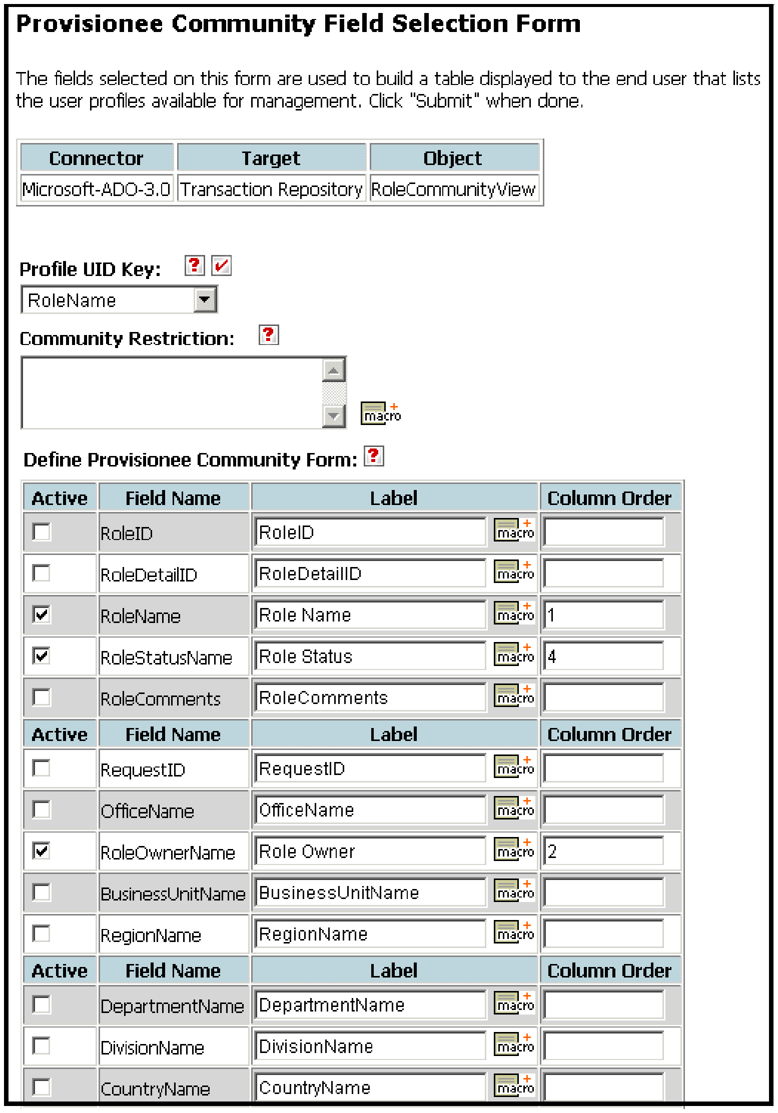
5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.
7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Provisionee Refine Search Form, can help the provisioner limit the number of returned profiles (see *“Refine the List of Displayed Provisionee Profiles” on page 176*).

9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Provisionee Refine Search Form to display profiles that more closely match search criteria.
10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message will display if the provisioner has entered values on the Provisionee Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Provisionee Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label for Community Display** text box appears as a title over the Mining Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Leave the **Select Connector** drop-down list box set to Microsoft ADO, the **Select Target** drop-down list box set to Transaction repository, and the **Object** drop-down list box set to RoleCommunityView.
14. Click **Configure...**.

    The Administration Manager displays the Define Provisionee Community Field Selection Form, shown in *Figure 89*.

    Note: The list of fields has been shortened to save space.

Figure 89: Define Provisionee Community Field Selection Form



Provisionee Community Field Selection Form

The fields selected on this form are used to build a table displayed to the end user that lists the user profiles available for management. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADO-3.0	Transaction Repository	RoleCommunityView

Profile UID Key:

RoleName

Community Restriction:

macro

Define Provisionee Community Form:

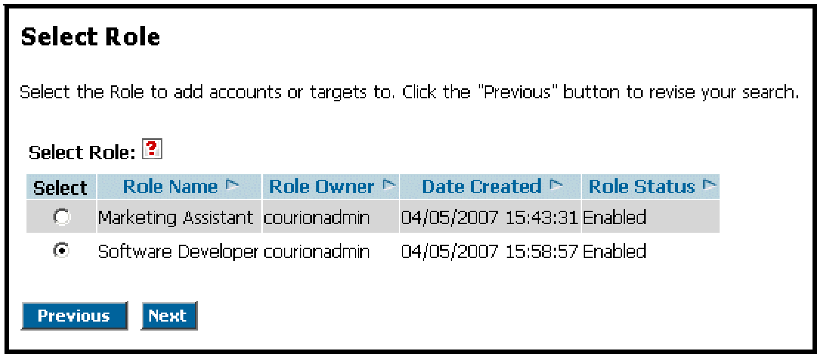
Active	Field Name	Label	Column Order
☐	RoleID	RoleID	
☐	RoleDetailID	RoleDetailID	
☑	RoleName	Role Name	1
☑	RoleStatusName	Role Status	4
☐	RoleComments	RoleComments	
Active	**Field Name**	**Label**	**Column Order**
☐	RequestID	RequestID	
☐	OfficeName	OfficeName	
☑	RoleOwnerName	Role Owner	2
☐	BusinessUnitName	BusinessUnitName	
☐	RegionName	RegionName	
Active	**Field Name**	**Label**	**Column Order**
☐	DepartmentName	DepartmentName	
☐	DivisionName	DivisionName	
☐	CountryName	CountryName	

15. In the **PROFILE UID KEY** drop-down box, leave the value set to RoleName.
16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Statement syntax depends on the target datasource. Do not use hashed or encrypted fields in the statement.

    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on Defining a Dynamic Community.
17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner.
18. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change “EmployeeBadgeNumber” field to “Badge number:”.
19. In the **COLUMN ORDER** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered “1” appears as the first column.
20. Click **SUBMIT**.

Figure 90 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 90: Select Role Screen



Refine the List of Displayed Mining Profiles

The Courion Role Creation sample workflow uses the Mining Community to select a group of users whose account access most closely matches the role that you want to add additional template accounts to.

By default, RoleCourier displays all the users to the provisioner that meet the criteria configured in the Define Mining Community Form. If the filtering criteria for the Define Mining Community Form are broad or the company is large, the community of users can be extensive. You can select one or more fields to include on a Mining Refine Search Form. These fields are presented to the provisioner. The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of users that meet the Mining Refine Search criteria. The provisioner then selects a user from the list to be used for mining.

The provisioner can choose to skip entering data on this form. If the form is skipped, RoleCourier returns all the user profiles established by the Define Mining Community Form.

To modify the Mining Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Mining Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Mining Refine Search**.

The process to refine the list of displayed profiles from a Mining Community in the Add Action of the Role Creation workflow is the same as for a Create Action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Define a Mining Community

The Mining Community is a set of existing users in a database or directory whose attributes may be used as a model for selecting attributes for an account that is being provisioned. The provisioner selects one or more users.

Note: The Mining Community is global and affects all actions within a workflow. Therefore, any changes made will apply to both the Create and Add actions in the Role Creation workflow.

Note: For the Mining Community to be displayed to the provisioner, the **Show Mining Community** on the Properties form must be selected. (This field is selected by default in the Role Creation workflow.)

Note: To use the Mining functionality, at least one attribute must have the **Mining** option selected in the **Presentation** field on the Unique Target Data Field Selection Form. See *"Specify Unique Resource Data Fields for the Target" on page 168* for details.

To modify the Define Mining Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Mining Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Mining Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Mining Community**.

The process to configure the Mining Community for an Add Action is the same as for a Create Action.

To modify the Mining Community Form and the forms that follow, complete the steps described in *"Define a Mining Community" on page 152*.

Refine the List of Displayed Resource Profiles

The Courion Role Creation sample workflow uses the Resource Community to select a baseline user account as a model for adding template accounts to the role.

By default, RoleCourier displays all the users to the provisioner that meet the criteria configured in the Define Resource Community Form. If the filtering criteria for the Define Resource Community Form are broad or the company is large, the community of users could be extensive. You can select one or more fields to include on a Resource Refine Search Form. These fields are presented to the provisioner. The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of users that meet the Resource Refine Search criteria. The provisioner then selects a user from the list as a model.

The provisioner can choose to skip entering data on this form. If the form is skipped, RoleCourier returns all the user profiles established by the Define Resource Community Form. See *“Define a Resource Community” on page 184*.

To modify the Resource Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Resource Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Resource Refine Search**.

The process to modify the Resource Refine Search in the Add Action of the Role Creation workflow is the same as for a Create Action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Define a Resource Community

The Add action in the Courion Role Creation sample workflow uses the Resource Community to select a baseline user account as a model for selecting additional template accounts that can be added to the role. It is important to choose a baseline user account that has the target accounts that you want to add to the role, or you will not be able to add those targets.

By using the Community Restriction parameter, found on the Resource Community Field Selection Form, you can restrict the resources that the provisioner can access. For example, you can set up a list that includes only the members of the Engineering department and restrict the provisioner to only provisioning resources associated with those members of the Engineering Department.

In practice, the Community Restriction parameter is often used to select a single baseline user. This ensures that all necessary targets are available for the role. In this case, you can select the **Automate selection of resource community when only one source user is available** checkbox on the Properties Form, to enable automatic selection of the source profile (and bypass both the Resource Community and resource Refine Search screens).

Note: The Resource Community is global and affects all actions within a workflow. Therefore, any changes made will apply to both the Create and Add actions in the Role Creation workflow.

To modify the Define Resource Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Resource Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Resource Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Resource Community**.

The process to configure the Resource Community for an Add Action is the same as for a Create Action.

To complete the Resource Community Form and the forms that follow, complete the steps described in *“Define a Resource Community” on page 159*.

Define the IdentityMap Screen Presentation for the Add Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Add to Role Screen, shown in *Figure 91*.

Note: If the **Automate selection of IdentityMap** on the Properties form is enabled, this form is skipped in the workflow, all of the baseline user’s accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter Account Attributes for Role screen to the provisioner).

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the navigation bar.
4. Click on **Add Request** and click on **IdentityMap Screen**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions**, expand **Add**, and expand **Action Settings**.
4. Click the icon next to **IdentityMap Screen**.

The process to modify the fields for the IdentityMap Screen in the Add action of the Role Creation workflow is the same as for an Add action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

In the example *Figure 91*, a Remedy account is being added to the role. In the Courion Role Creation sample workflow there are two tabs, labelled “Corporate Systems” and “Role Management”. The labels for these tabs are determined by the values chosen in the **Category** field found on the Add and Modify Target forms. Targets configured with the same category name will show up under a single tab. If no category is specified, the target will show up under a tab labelled “Accounts”. In this example, the Remedy target was not assigned a category, so it shows up under the “Accounts” tab. (For more details on configuring targets, see *Table 5 on page 245*.)

In the case of the sample workflow, the Courion Role Connector has been given its own separate category to help distinguish that this target is used for creation of the role itself, whereas the other targets are used to create template accounts that link to the role.

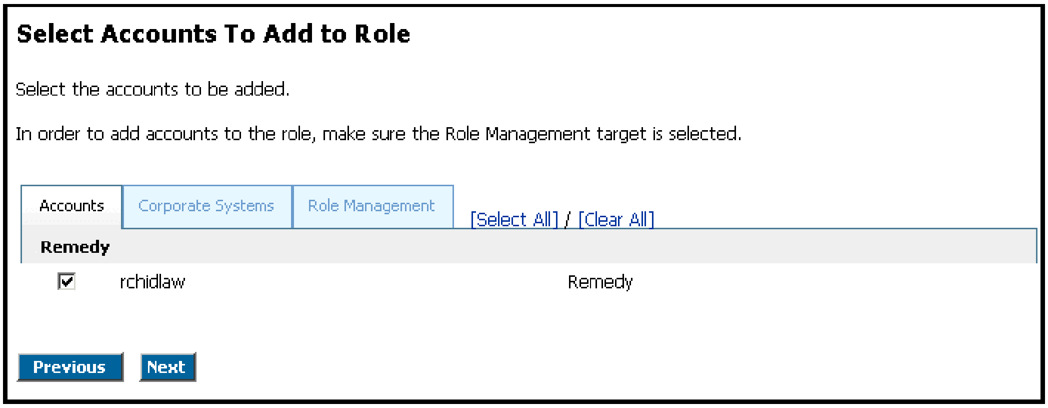
The names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. If one or more users have been selected from the mining community, both a resource description and a popularity indicator are displayed above the resource name, checkbox, and target name. The description is taken from the **Description** field on the Add and Modify Target forms. If no mining users are selected, only the resource name, checkbox, and target name are displayed. As shown in *Figure 78*, the description can include a graphic.

In addition to the Role Management target, the targets that are displayed are determined by the accounts owned by the user selected as the baseline. (The targets must also be configured on the Target Configuration Form.) For each target listed under a tab, the provisioner must select the target by checking the checkbox, if they want to create a template account for that target.

In the Add action of the Role Creation workflow, the Role Management target is selected automatically and may not be unselected. (If not selected, the template account would not be linked to the role.) This is determined by the RoleSampleIDMap.xslt file assigned in the **XSLT File for Processing** field.

Figure 91: Select Accounts to Add Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Resource Data form to configure which attributes are used to provision the template accounts that are linked to the role. The Unique Target Data form displays the currently available targets for which template accounts can be created. The Courion Role Creation sample workflow has three targets already configured—the Role Repository (for creation of the role itself), Active Directory (for a logon ID), and Microsoft Exchange (for an email account). If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. For more details on configuring targets, see *Table 5 on page 245*.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which will display mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Creation** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Add** from the **Action** drop-down menu.
4. Click on **Add Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Creation** workflow.
3. Expand **Actions** and expand **Add**.
4. Click the icon next to **Unique Resource Data**.

The steps to complete the Unique Target Data Form to add a resource are the same as to create a resource. Follow the instructions provided in *“Specify Unique Resource Data Fields for the Target” on page 168*.

Chapter 9: Configuring a Role Lifecycle Management Workflow

This chapter describes how to configure a workflow to manage roles and template accounts associated with those roles, using the Courion Role Management sample workflow as a model.

The Role Management sample workflow uses the Create, Change, Delete, Disable, and Enable actions to create a role using an existing role as a model, and to manage the lifecycle of that role. If you are creating roles for the first time, you need to use the Courion Role Creation sample workflow. See *"Configuring a Role Creation Workflow" on page 145* for details.

Role Management Actions:

- **Create** a new role. Although both the Role Management sample workflow and the Courion Role Creation workflow offer the Create action as an option, the Role Management workflow differs from the Role Creation workflow in that it uses existing roles for the Mining community, while the Role Creation workflow mines individual user accounts.
- **Change** the attribute values for the template accounts associated with a role
- **Delete** the template accounts associated with a role
- **Enable** and **Disable** the roles and/or the template accounts associated with a role

The sections in this chapter use the Courion Role Management sample workflow, providing practical examples of how to configure RoleCourier workflows:

- *"Details on Global Settings Specific to the Role Management Workflow" on page 190* describes information specific to this workflow.
- *"Creating a Role Based on Existing Roles" on page 191* describes using the Courion Role Management sample workflow to create a new role and associated template accounts by mining other existing roles.
- *"Change Account Attributes for an Existing Role" on page 215* describes using the Courion Role Management sample workflow to change the attributes of a role or it's template accounts or both.
- *"Disabling and Enabling a Role and its Template Accounts" on page 228* describes using the Courion Role Management sample workflow to disable or enable the a role or it's template accounts or both.
- *"Deleting the Template Accounts for a Role" on page 236* describes using the Courion Role Management sample workflow to delete the template accounts associated with a role.

Details on Global Settings Specific to the Role Management Workflow

When the sample workflows are installed during Express Configuration, a number of forms are pre-configured that are not described in this manual. You can modify these forms based on your specific needs. An overview of these forms, applying to all the sample workflows, is described in *“Global Settings” on page 13*.

Additionally, the following information is specific to the Courion Role Management workflow:

Transaction Repository

The Role Management workflow uses the transaction repository to store information about the role. It also contains the IdentityMap information. It uses the Microsoft ADO connector. For details, see *Table 5 on page 245*.

The Courion Role Connector takes data that is persisted with every provisioning transaction (Request), and adds definitional information to indicate to the system that this data is now a role definition, as opposed to the record of a request. It stores the persisted data in the transaction repository.

To the transaction repository, a role is an entity that consists of a collection of targets. Each target can have a collection of accounts, and each account can have a collection of attribute/value pairs. This data is collected whenever a Request is submitted to the transaction repository. If the Courion Role Connector is one of the targets in a provisioning action, it undertakes the necessary back-end data transformations to convert a normal request into a role definition. All data exposed on all targets (whether hidden or visible), becomes part of the role definition.

For details on the schema available to define roles, see the appendix “Transaction Repository Database Views” in the manual *“Configuring Workflows with the Enterprise Provisioning Suite Administration Manager”*:

Macros

The Role Management workflow uses custom macros which substitute information gathered dynamically by the Courion Server into forms and messages displayed to the end user. Some of the custom macros were created for the Add action, to retrieve role information about the role to which accounts are being added.

These macros all begin with `RoleInfo:`*xxx*, where xxx is the attribute. For example, `RoleInfo:DepartmentName` returns the department assigned to the role.

Unused Forms in the Role Management Workflow

The following forms are not used in this workflow: Seed Refine Search, Seed Community, Role Refine Search, Role Community, Approval Community, Delegation Community, Password Synchronization, Resource Claiming, Resource Suggestions, Conditions, Account ID Generation.

Creating a Role Based on Existing Roles

This section describes how to configure the Create action, using the Courion Role Management sample workflow.

With this workflow, a provisioner creates a role record that is stored in the transaction repository, plus one or more template accounts on target systems that are associated with the role. The Role Management workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Use the Mining Community to select a group of roles whose account access most closely matches the role being created.
3. Select a single role to serve as the baseline for the role.
4. Select the individual attributes for each target associated with the role. For the attribute values, provisioners can view the values belonging to the members of the mining community, helping them to select appropriate values for the template accounts.

Note: Since the Role Management workflow uses other roles for the mining community and the baseline, you must create at least a few roles using the Courion Role Creation workflow before you can use the Role Management workflow.

The following sections describe configuration of the forms needed for the Create action:

- *"Configure Properties for the Create Action" on page 192* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Mining Profiles" on page 194* describes how to set up a form that the user can complete to filter the mining profiles available in the workflow's community.
- *"Define a Mining Community" on page 195* describes how to set up a form that displays a table of users whose attributes can be "mined". The mined attributes are then displayed, enabling a provisioner to model attributes based on a group of users in stead of a single user.
- *"Refine the List of Displayed Resource Profiles" on page 199* describes how to set up a form the provisioner can complete to filter the resource profiles available in the workflow's community.
- *"Define a Resource Community" on page 200* describes how to set up a form that displays the roles available for modeling. The provisioner selects a role and the provisioning application uses the unique identifier in the role profile to search the IdentityMap for all the template accounts associated with the role.
- *"Define the IdentityMap Screen Presentation for the Create Action" on page 205* describes how to set up a form that controls the appearance of the Select Resources to Create form presented to the provisioner.
- *"Configure an Initial Profile" on page 207* describes how to set up a form the provisioner completes that specifies the fields required to create a basic profile record for the role.
- *"Specify Unique Resource Data Fields for the Target" on page 210* describes how to set up a form the provisioner completes that specifies the fields, and possible default values, required to create the new role.

The following instructions describe how to modify the settings in the Courion Role Management workflow. If you have created a new workflow by copying Courion Role Management, modify the forms in that workflow. See *“Copying Sample Workflows” on page 241* for information about how to create a new workflow by copying an existing workflow.

Configure Properties for the Create Action

To modify the Properties for Create Action Form:

Flowchart View

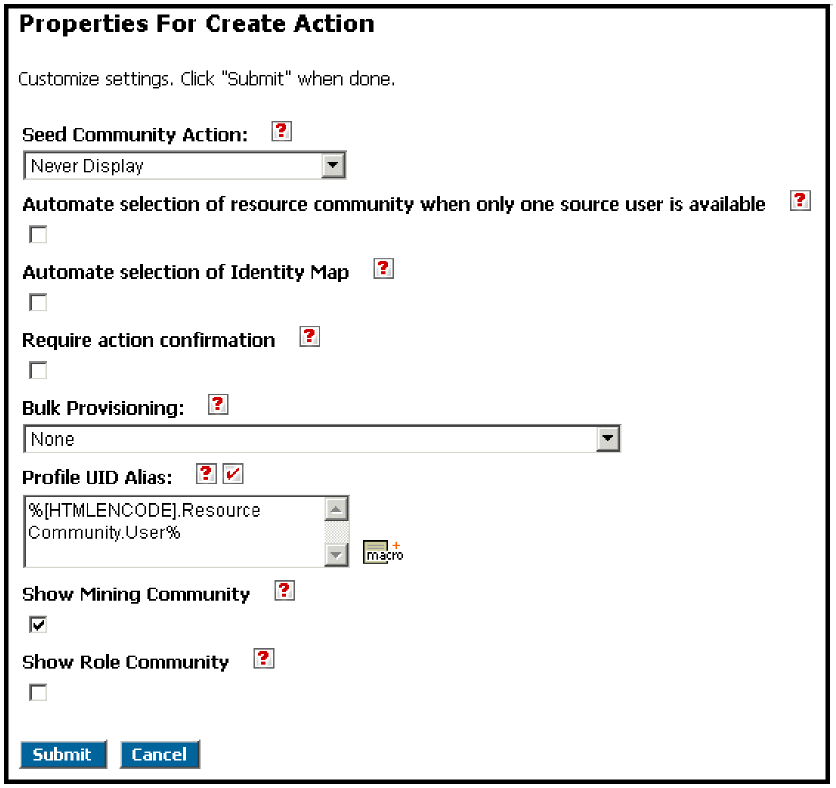
1. Log in to the Administration Manager Flowchart View.
2. Select **COURION ROLE MANAGEMENT** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CREATE** from the **ACTION** drop-down menu.
4. Click on **CREATE REQUEST**.
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS** and expand **CREATE**.
4. Click the  icon next to **PROPERTIES**.

   The Administration Manager displays the Properties for Create Action Form, shown in *Figure 92*.

Figure 92: Properties for Create Action Form



5. Leave the **Seed Community Action** option set to the default of Never Display. This workflow does not use the Seed Community.

6. Select the **Automate selection of resource community when only one source user is available** checkbox to enable automatic selection of the source profile (and bypass the Resource Community screen) when only a single source profile is retrieved from the connector. This setting is not selected by default.

   If you have created a special account as a baseline, check this checkbox. If you want the provisioner to be able to choose the baseline from a group of user accounts, leave the checkbox unchecked.

7. Select the **Automate selection of IdentityMap** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **Submit** button. This setting is turned off by default.

   In this workflow, the Resource Community is used to select a role as the baseline. Therefore, if this checkbox is selected, all of the baseline role's accounts are selected and template accounts for the new role are created on all those targets.

8. Select the **Require action confirmation** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.

9. Leave the **Bulk Provisioning** option set to the default of None. This workflow does not use Bulk Provisioning.

10. The **Profile UID Alias** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the Courion Role Management sample workflow, this is set to %[HTMLENCODE].Resource Community.User%.

11. Leave the **Show Mining Community** checkbox selected since this workflow uses the mining community.
12. Leave the **Show Role Community** checkbox unselected since this workflow does not use the role community.
13. Click **Submit**.

Refine the List of Displayed Mining Profiles

The Courion Role Management sample workflow uses the Mining Community to select a group of roles whose account access most closely matches the role that is being created.

By default, RoleCourier displays all the roles to the provisioner that meet the criteria configured in the Define Mining Community Form. If the filtering criteria for the Define Mining Community Form are broad or the company is large, the community of roles can be extensive. You can select one or more fields to include on a Mining Refine Search Form. These fields are presented to the provisioner on the Search for Mining Community Candidates screen (*Figure 93*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of roles that meet the Mining Refine Search criteria. The provisioner then selects one or more roles from the list to be used for mining.

The provisioner can choose to skip entering data on the Search for Mining Community Candidates screen. If the screen is skipped, RoleCourier returns all the user profiles established by the Define Mining Community Form. You may also configure Mining Refine Search Form so that the Search for Mining Community Candidates screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Mining Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Mining Refine Search**.

Tree View

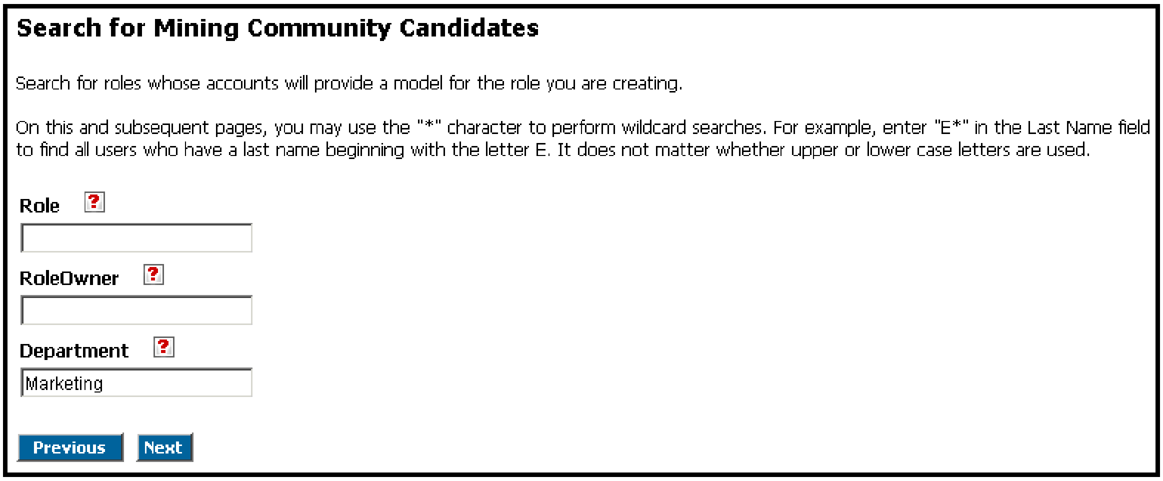
1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the icon next to **Mining Refine Search**.

The process to refine the list of displayed profiles from a Mining Community in the Create action of the Role Management workflow is the same as for a Create action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Figure 93 shows the screen displayed to provisioner, based on the settings from the Role Management workflow.

Figure 93: Refine Mining Community Search Screen



Define a Mining Community

The Mining Community is a set of existing entities in a database or directory whose attributes may be used as a model for selecting attributes for an account that is being provisioned. Although in many cases the Mining Community consists of users, in the case of the role Management workflow, the Mining Community consists of other roles.

Note: The Mining Community is global and affects all actions within a workflow. Therefore, any changes made will apply to all the actions in the Role Management workflow.

Note: For the Mining Community to be displayed to the provisioner, you must select the **Show Mining Community** option on the Properties form. (This field is selected by default in the Role Management workflow.)

Note: To use the Mining functionality, at least one attribute must have the **Mining** option selected in the **Presentation** field on the Unique Target Data Field Selection Form. See *"Specify Unique Resource Data Fields for the Target" on page 210* for details.

To modify the Define Mining Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Mining Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.

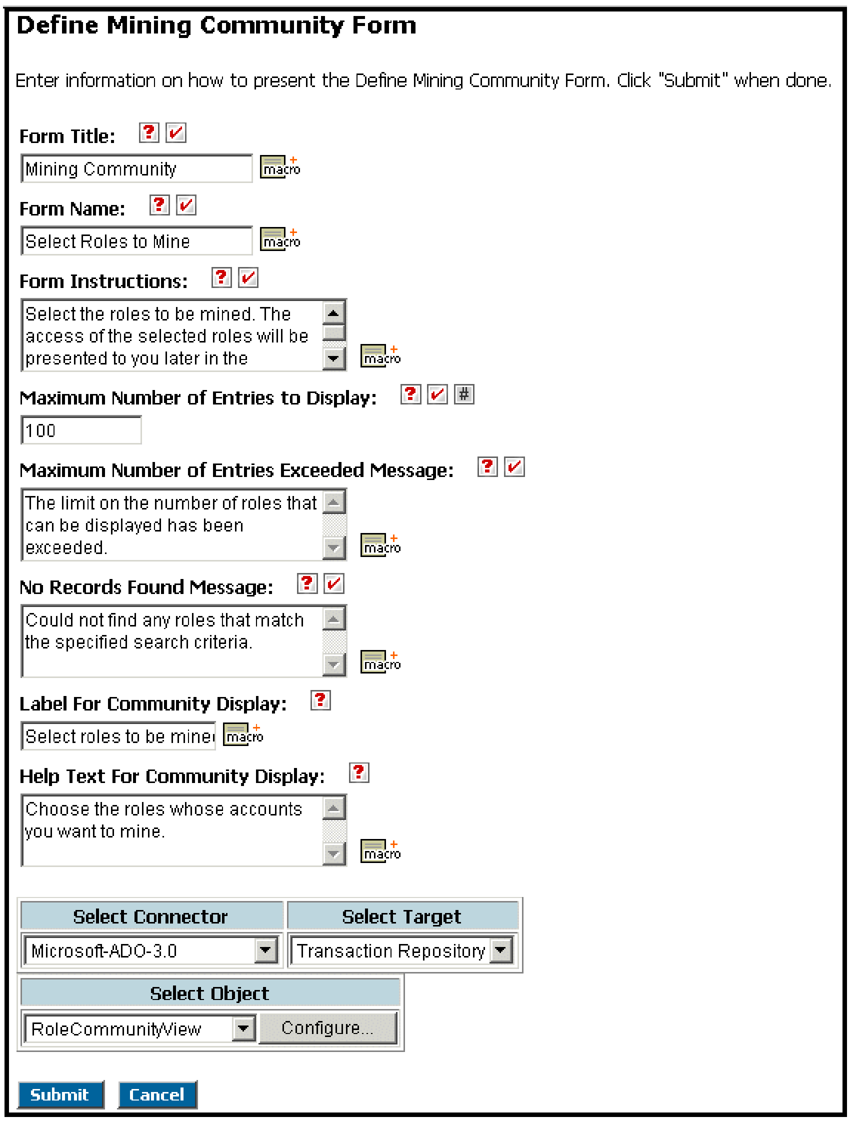
4. Click on **Mining Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Mining Community**.

   The Administration Manager displays the Define Mining Community Form, shown in *Figure 94* with default text and sample data. You can edit all text boxes.

Figure 94: Define Mining Community Form


Define Mining Community Form

Enter information on how to present the Define Mining Community Form. Click "Submit" when done.

Form Title:
Mining Community

Form Name:
Select Roles to Mine

Form Instructions:
Select the roles to be mined. The access of the selected roles will be presented to you later in the

Maximum Number of Entries to Display:
100

Maximum Number of Entries Exceeded Message:
The limit on the number of roles that can be displayed has been exceeded.

No Records Found Message:
Could not find any roles that match the specified search criteria.

Label For Community Display:
Select roles to be mine

Help Text For Community Display:
Choose the roles whose accounts you want to mine.

Select Connector	Select Target
Microsoft-ADO-3.0	Transaction Repository

Select Object
RoleCommunityView Configure...

Submit Cancel

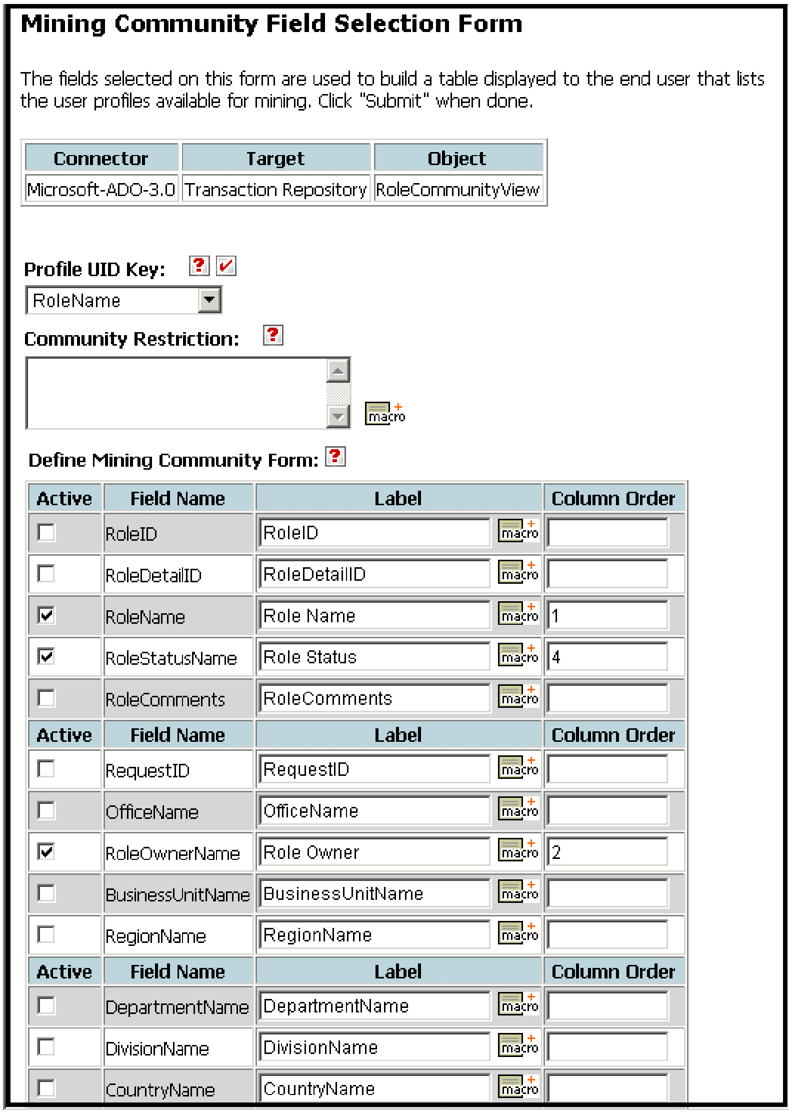
5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.

7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Mining Refine Search Form, can help the provisioner limit the number of returned profiles (see *“Refine the List of Displayed Mining Profiles” on page 194*).
9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Mining Refine Search Form to display profiles that more closely match search criteria.
10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message will display if the provisioner has entered values on the Mining Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Mining Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label For Community Display** text box appears as a title over the Mining Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Leave the **Select Connector**, **Select Target**, and **Object** fields set to their default values. The sample workflow uses the RoleCommunityView in the Transaction repository to access the role info.
14. Click **Configure...**.

    The Administration Manager displays the Define Mining Community Field Selection Form, shown in *Figure 95*.

Note: The fields displayed on the form depend on the object selected. The list of fields has been shortened to save space.

Figure 95: Define Mining Community Field Selection Form



Mining Community Field Selection Form

The fields selected on this form are used to build a table displayed to the end user that lists the user profiles available for mining. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADO-3.0	Transaction Repository	RoleCommunityView

Profile UID Key:

RoleName

Community Restriction:

Define Mining Community Form:

Active	Field Name	Label	Column Order
☐	RoleID	RoleID	
☐	RoleDetailID	RoleDetailID	
☑	RoleName	Role Name	1
☑	RoleStatusName	Role Status	4
☐	RoleComments	RoleComments	
Active	**Field Name**	**Label**	**Column Order**
☐	RequestID	RequestID	
☐	OfficeName	OfficeName	
☑	RoleOwnerName	Role Owner	2
☐	BusinessUnitName	BusinessUnitName	
☐	RegionName	RegionName	
Active	**Field Name**	**Label**	**Column Order**
☐	DepartmentName	DepartmentName	
☐	DivisionName	DivisionName	
☐	CountryName	CountryName	

15. In the **PROFILE UID KEY** drop-down box, select the unique user ID field in this object that will serve as a link to a user's entries, identified by the Profile UID field, in the Resource Community table.

16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Statement syntax depends on the target datasource. Do not use hashed or encrypted fields in the statement.

    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on defining a Dynamic Community.

17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner.

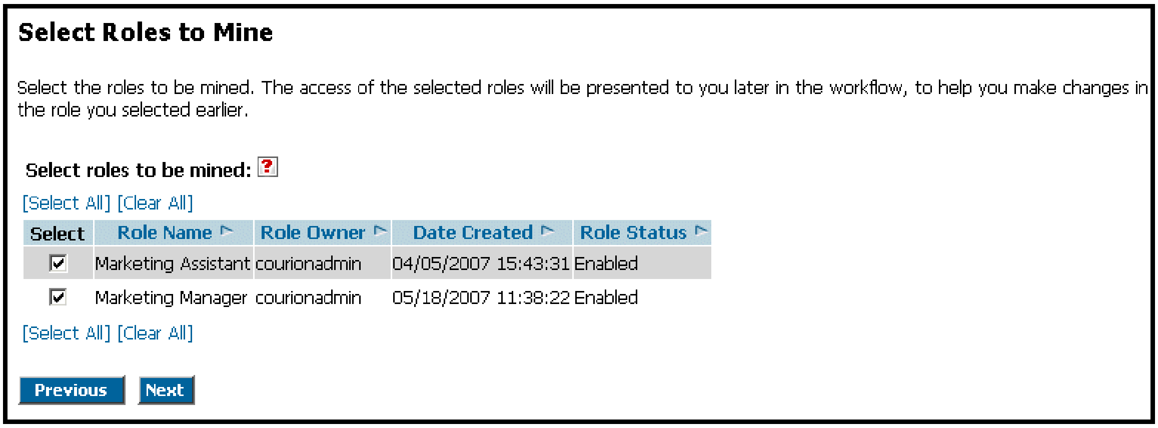
18. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change "EmployeeBadgeNumber" field to "Badge number:".

19. In the **Column Order** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered “1” appears as the first column.

20. Click **Submit**.

Figure 96 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 96: Select Roles to Mine Screen



Refine the List of Displayed Resource Profiles

The Courion Role Management sample workflow uses the Resource Community to select a baseline role account as a model for creating the role.

By default, RoleCourier displays all the roles to the provisioner that meet the criteria configured in the Define Resource Community Form. If the filtering criteria for the Define Resource Community Form are broad or the company is large, the community of roles could be extensive. You can select one or more fields to include on a Resource Refine Search Form. These fields are presented to the provisioner on the Search for Role Baseline Candidates screen (*Figure 97*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of roles that meet the Resource Refine Search criteria. The provisioner then selects a role from the list as a model.

The provisioner can choose to skip entering data on the Search for Role Baseline Candidates screen. If the screen is skipped, RoleCourier returns all the role profiles established by the Define Resource Community Form. You may also configure Resource Refine Search Form so that the Search for Role Baseline Candidates screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Resource Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Resource Refine Search**.

Tree View

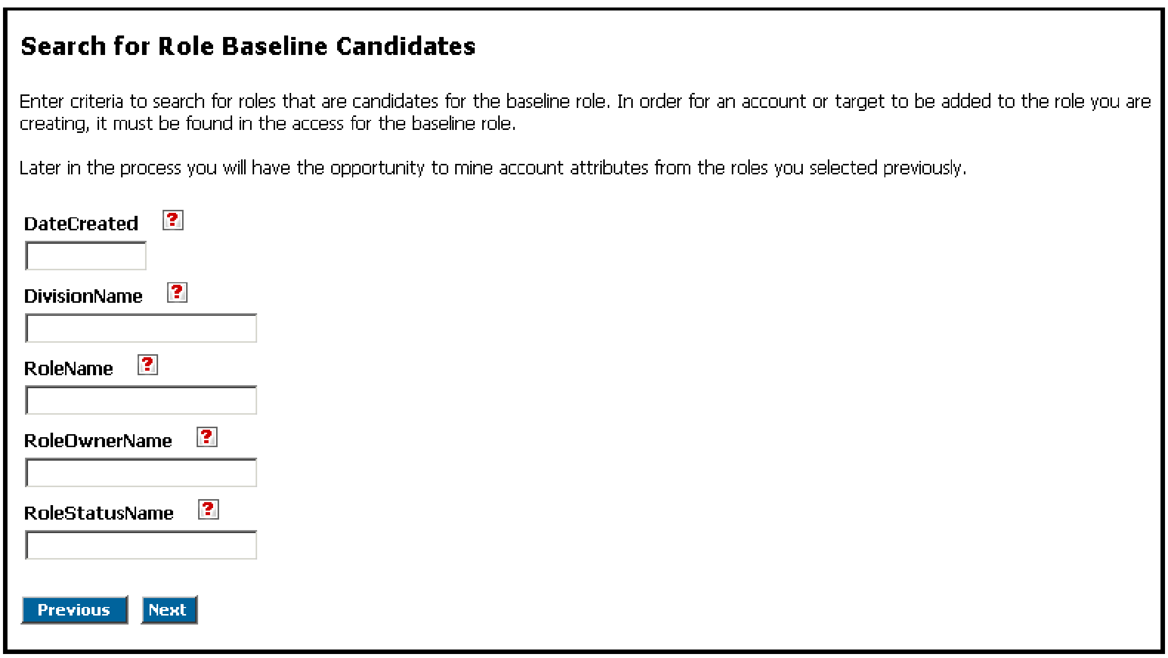
1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS** and expand **CREATE**.
4. Click the icon next to **RESOURCE REFINE SEARCH**.

The process to refine the list of displayed profiles from a Resource Community in the Create action of the Role Management workflow is the same as for a Create action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Figure 97 shows the screen displayed to provisioner, based on the settings from the Role Management workflow.

Figure 97: Search for Role Baseline Candidates Screen



Define a Resource Community

The Courion Role Management sample workflow uses the Resource Community to select a baseline role as a model for creating the new role. The workflow then creates a role record that is stored in the transaction repository, plus one or more template accounts on target systems that are associated with the role. It is important to choose a baseline role that has all the target accounts that you want to associate with the role, since additional targets can not be added in the workflow. (You can, however, use the Add to an Existing Role action in the Courion Role Creation workflow to add additional targets. See *"Adding to an Existing Role" on page 173* for details.)

By using the Community Restriction parameter, found on the Resource Community Field Selection Form, you can restrict the resources that the provisioner can access. For example, you can set up a list that includes only the members of the Marketing department and restrict the provisioner to only provisioning resources associated with those members of the Marketing department.

In practice, the Community Restriction parameter is often used to select a single baseline user. This ensures that all necessary targets are available for the role. In this case, you can select the **Automate selection of resource community when only one source user is available** checkbox on the Properties Form, to enable automatic selection of the source profile (and bypass both the Resource Community and resource Refine Search screens).

Note: The Resource Community is global and affects all actions within a workflow. Therefore, any changes made will apply to both the Create and Add actions in the Role Management workflow.

To modify the Define Resource Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Resource Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

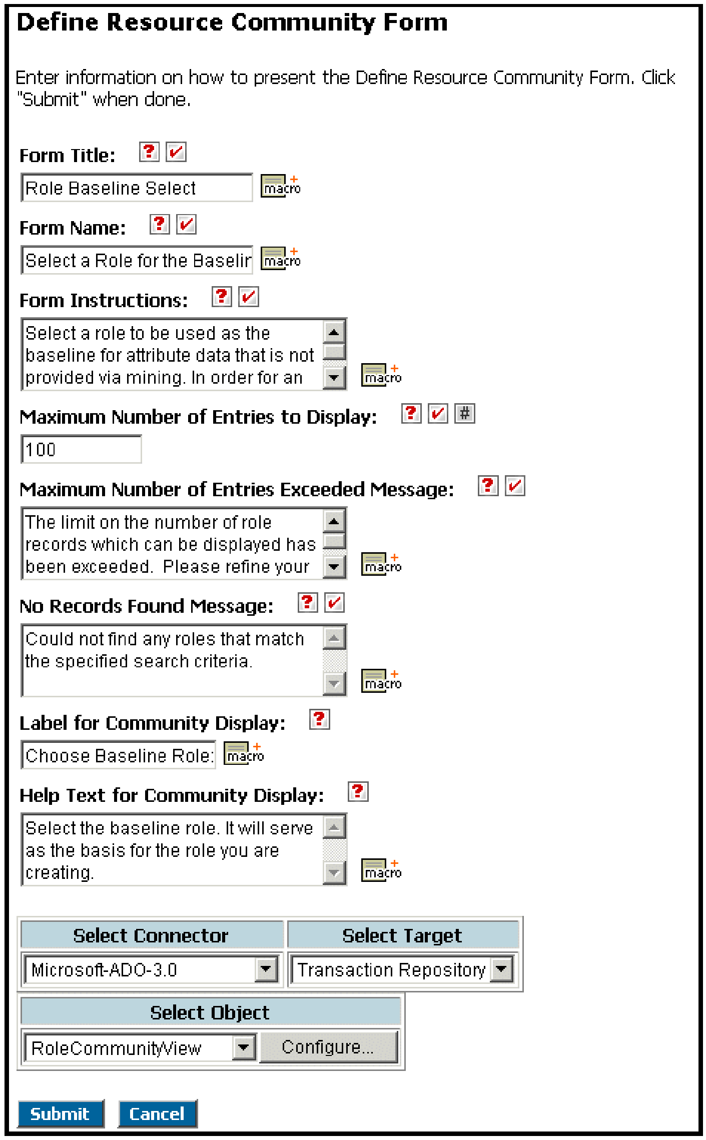
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Resource Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Global Settings**.
4. Click the icon next to **Resource Community**.

The Administration Manager displays the Define Resource Community Form, shown in *Figure 98* with default text and sample data. All text boxes can be edited.

Figure 98: Define Resource Community Form



5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.
7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the "<" and ">" is considered an HTML tag and is not displayed.)
8. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Source Refine List Form, can help the provisioner limit the number of returned profiles (see *"Refine the List of Displayed Resource Profiles" on page 199*).

9. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Source Refine Search Form to display profiles that more closely match search criteria.
10. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message will display if the provisioner has entered values on the Source Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Refine Search Form or to skip the form to return a list of all profiles in the community.
11. Text in the **Label for Community Display** text box appears as a title over the Resource Community list.
12. Text in the **Help Text For Community Display** describes the action to take in the community display.
13. Select a connector from the **Select Connector** drop-down list box. In the sample workflow, this is the Connector for Microsoft Active Directory.

    Select a target from the **Select Target** drop-down list box.

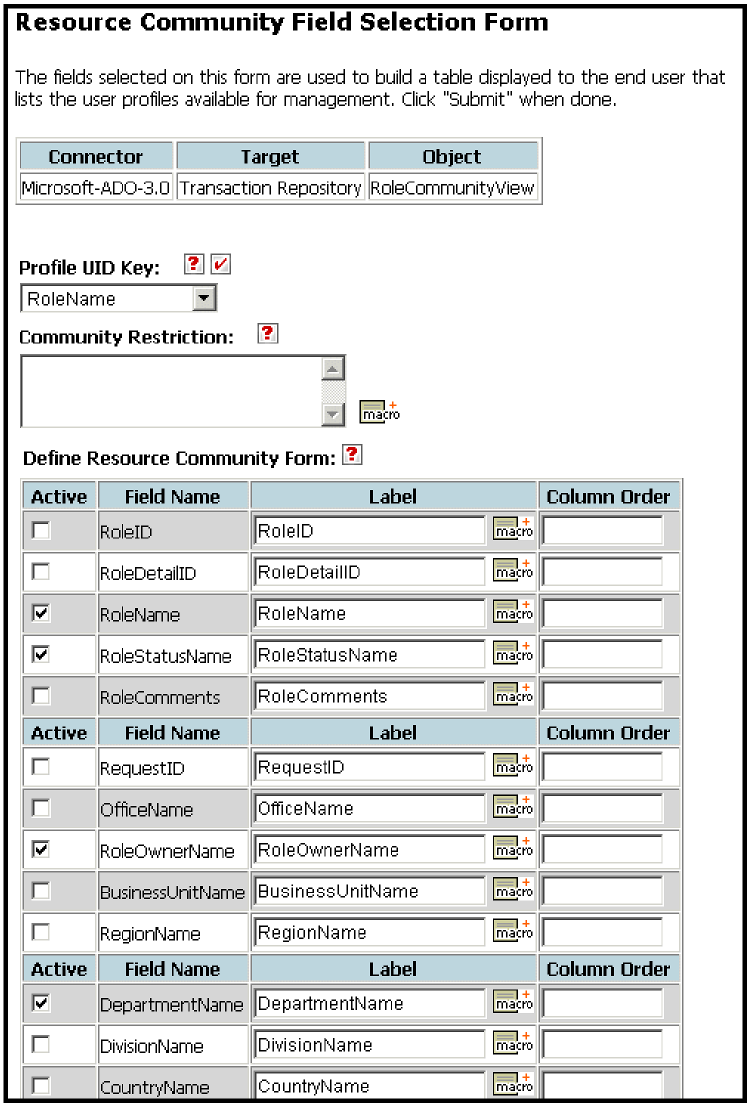
    Select an object from the **Object** drop-down list box.

    Note: The available connectors and targets depend on what has been provided through the Connector Configuration Manager. Collectively, the connector, target, and object point to the datasource that contains the user profiles available in this workflow.
14. Click **Configure...**.

    The Administration Manager displays the Resource Community Field Selection form, shown in *Figure 99*.

    Note: The fields displayed on the form depend on the object selected. The list of fields has been shortened to save space.

Figure 99: Resource Community Field Selection Form



15. In the **PROFILE UID KEY** drop-down box, select the unique user ID field in this object that will serve as a link to a user's entries, identified by the Profile UID field, in the Resource Community table.
16. In the **COMMUNITY RESTRICTION** text box, enter a statement to restrict the return of available profiles. Do not use hashed or encrypted fields in the statement.

    In the Role Management workflow, the macro restricts return of available profiles to Active Directory records that belong to users, and only those users with a profile stored in the IdentityMap.

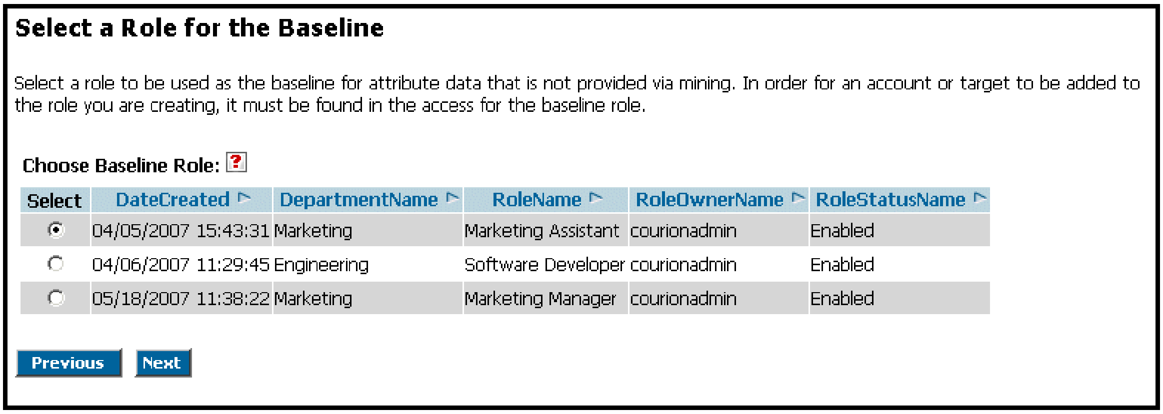
    You can set up a Dynamic Community to make a single workflow available to multiple provisioners. Refer to *Table 5 on page 245* for details on defining a Dynamic Community.
17. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change "EmployeeBadgeNumber" field to "Badge number:".

18. In the **Column Order** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered “1” appears as the first column.

19. Click **Submit**.

Figure 100 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 100: Select a Role for the Baseline Screen



Define the IdentityMap Screen Presentation for the Create Action

The IdentityMap Screen form controls the labels and formatting for the Select Resources to Create Screen, shown in *Figure 101*.

Note: If the **Automate selection of IdentityMap** on the Properties form is enabled, this form is skipped in the workflow, all of the baseline role’s template accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter Role Information screen to the provisioner).

To modify the IdentityMap Screen Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **IdentityMap Screen**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the icon next to **IdentityMap Screen**.

The process to modify the fields for the IdentityMap Screen in the Create action of the Role Management workflow is the same as for a Create action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

For the Select Resources to Create screen, in the Courion Role Management sample workflow you will see two tabs, labelled “Corporate Systems” and “Role Management”. The labels for these tabs are determined by the values chosen in the **CATEGORY** field found on the Add and Modify Target forms. Targets configured with the same category name will show up under a single tab. If no category is specified, the target will show up under a tab labelled “Accounts”. (For more details on configuring targets, see *Table 5 on page 245*.)

In the case of the sample workflow, the Courion Role Connector has been given its own separate category to help distinguish that this target is used for creation of the role itself, whereas the other targets are used to create template accounts that link to the role.

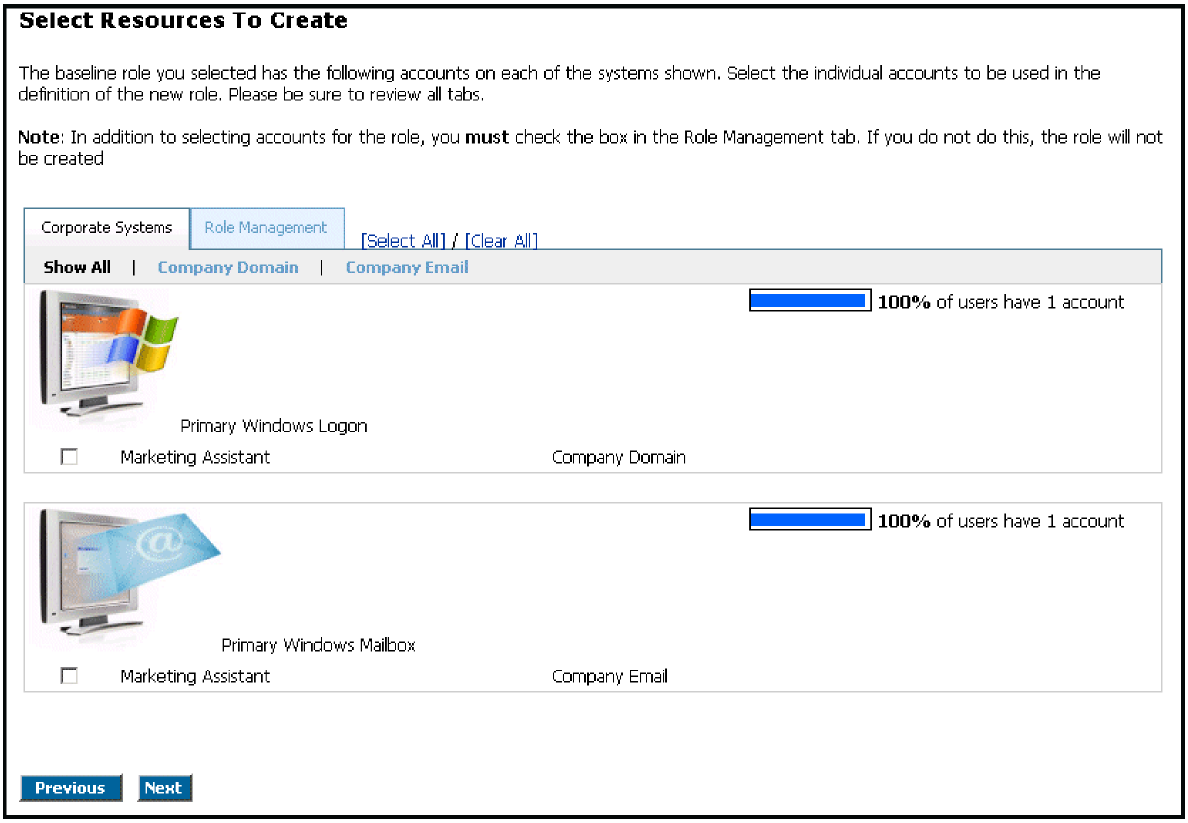
The names of the individual targets in the grey menu bar are taken from the **ALIAS** field on the Add and Modify Target forms. If no alias is specified, the **IDENTITYMAP TARGET ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. If one or more users have been selected from the mining community, both a resource description and a popularity indicator are displayed above the resource name, checkbox, and target name. The description is taken from the **DESCRIPTION** field on the Add and Modify Target forms. If no mining users are selected, only the resource name, checkbox, and target name are displayed. As shown in *Figure 101*, the description can include a graphic.

In addition to the Role Management target, the targets that are displayed are determined by the accounts owned by the role selected as the baseline. (The targets must also be configured on the Target Configuration Form.) For each target listed under a tab, the provisioner must select the target by checking the checkbox, if they want to create a template account for that target.

In the Role Management workflow, the Role Management target is selected automatically and may not be unselected. (If not selected, the role would not be created.) This is determined by the RoleSampleIDMap.xslt file assigned in the **XSLT FILE FOR PROCESSING** field.

Figure 101: Select Resources to Create Screen



Configure an Initial Profile

In the Courion Role Management sample workflow, the Initial Profile form is used to collect basic data about the role that is used when the role and associated template accounts are created. No actual profile is created, since that does not apply to the creation of a role.

To modify the Initial Profile Form:

Flowchart View

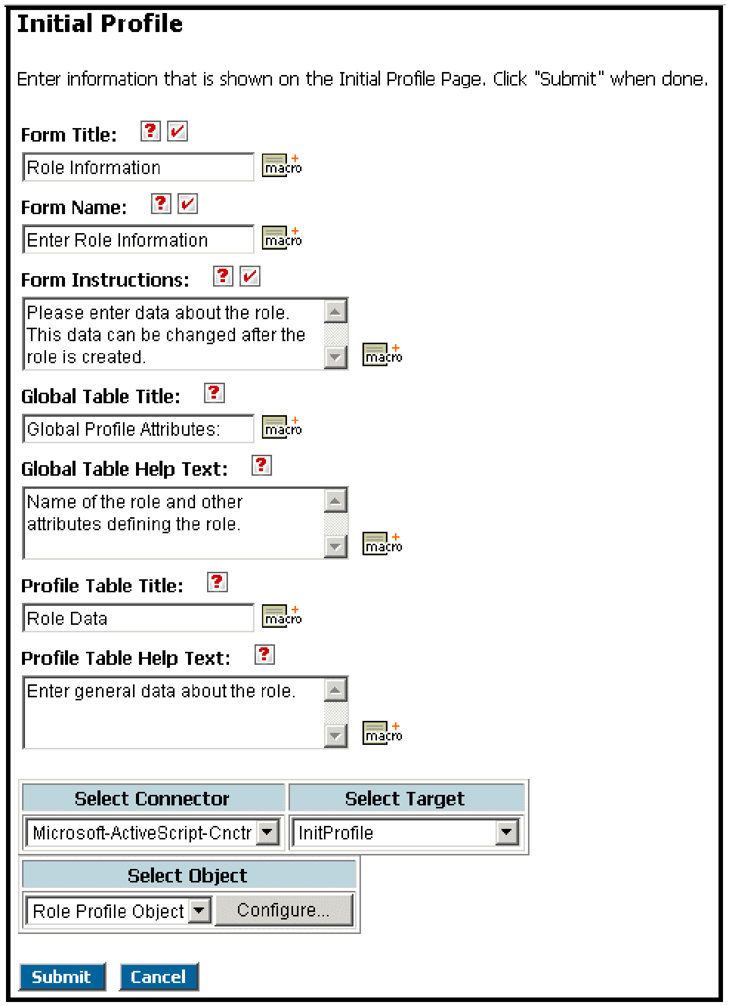
1. Log in to the Administration Manager Flowchart View.
2. Select **COURION ROLE MANAGEMENT** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CREATE** from the **ACTION** drop-down menu.
4. Click on **CREATE REQUEST**.
5. Click on **INITIAL PROFILE**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS** and expand **CREATE**.
4. Click the icon next to **INITIAL PROFILE**.

The Administration Manager displays the Initial Profile Form, shown in *Figure 102* with default text and sample data. All text boxes can be edited.

Figure 102: Initial Profile Form



5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.
7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. Text in the **Global Table Title** text box appears as the title on Global Fields Table.
9. Text in the **Global Table Help Text** box appears as the help text in the Global Fields Table.
10. Text in the **Profile Table Title** text box appears as the title for each user’s profile table.
11. Text in the **Profile Table Help Text** box appears as the help text in the Profile Table.
12. The **Select Connector**, **Select Target**, and **Select Object** fields are set to use a specific script for Microsoft Active Script, which prevents creation of a profile and passes the information collected here to the targets.

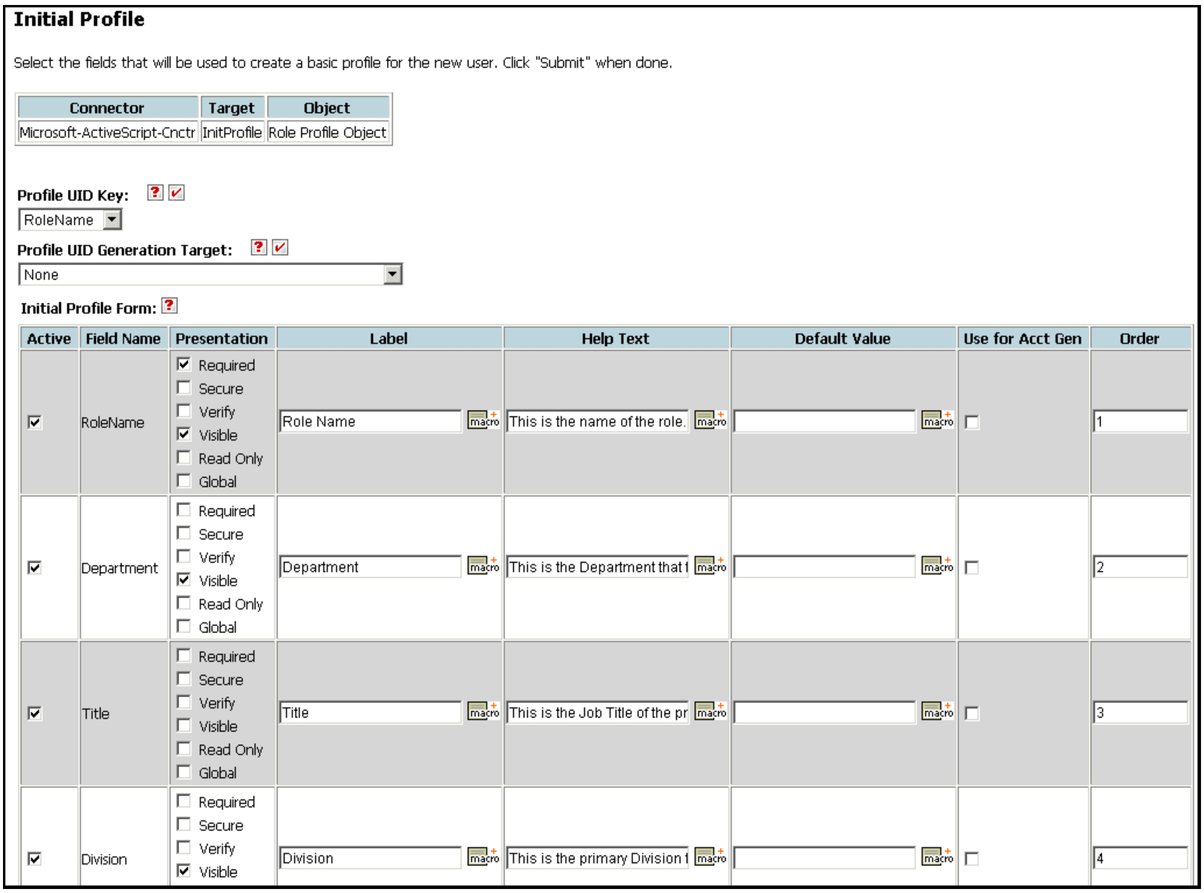
13. Click **CONFIGURE...**.

    The Administration Manager displays the Initial Profile Select Fields Form, shown in *Figure 103*.

    Note: The fields displayed depend on the object selected. The list of fields has been shortened to save space. *Figure 103* shows sample selections.

    Note: When creating an initial profile in Sun Directory Server, do not use the aci attribute. This attribute exceeds the maximum length for the field, causing the creation to fail.

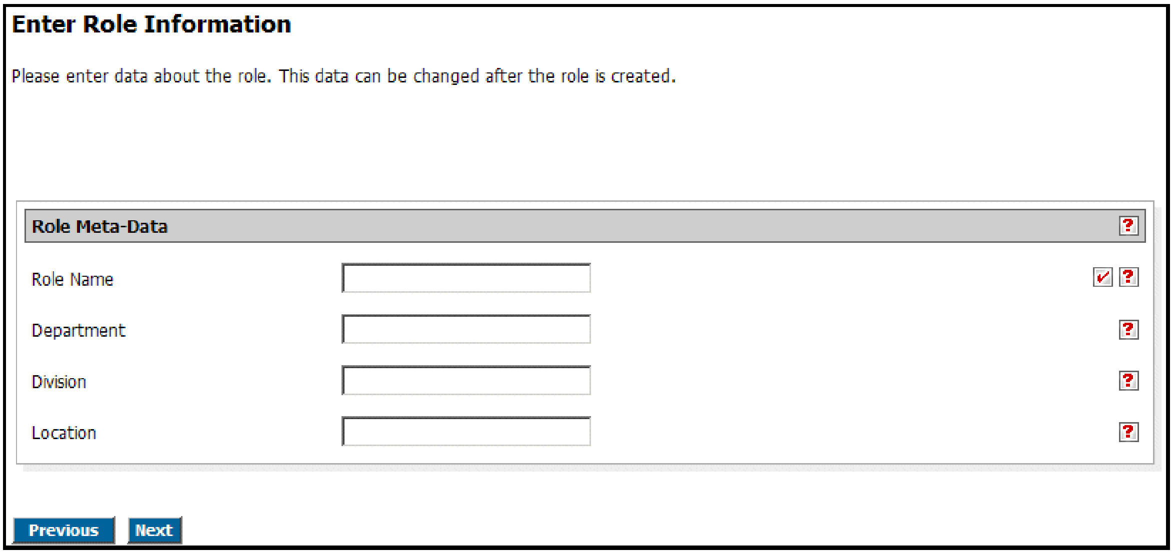
Figure 103: Initial Profile Select Fields Form



14. Select the fields to include in the initial profile for a new user. For a description of all fields, see *Table 2 on page 71*.
15. The **PROFILE UID KEY** drop-down box lists all configured targets for resource creation.
16. The **PROFILE UID GENERATION TARGET** drop-down box lists the targets whose generated resource names may be used as the Profile UID key.
17. Click **SUBMIT**.

Figure 104 shows an example of the Initial Profile form that the provisioner sees.

Figure 104: Enter Role Information Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are used to provision the template accounts that are linked to the role. The Unique Target Data form displays the currently available targets for which template accounts can be created. The Courion Role Management sample workflow has three targets already configured—the Role Repository (for creation of the role itself), Active Directory (for a logon ID), and Microsoft Exchange (for an email account). If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. Refer to *Table 5 on page 245* for information on this form.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which will display mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

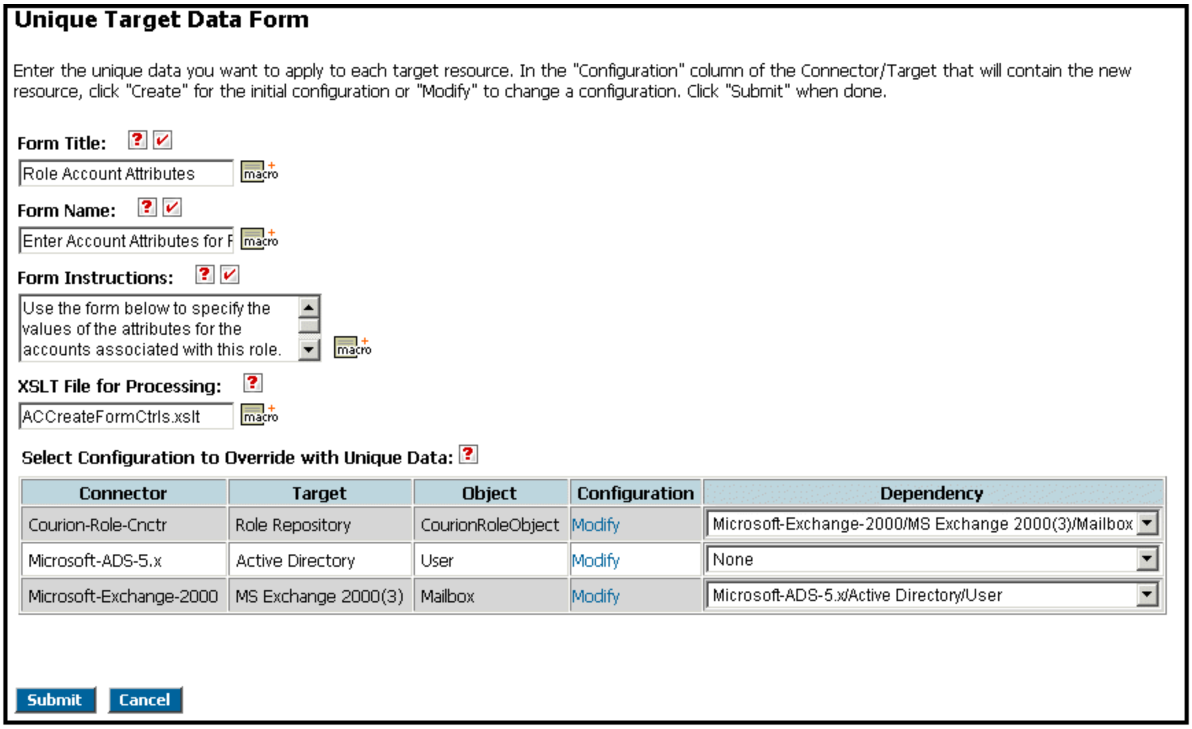
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Create** from the **Action** drop-down menu.
4. Click on **Create Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Create**.
4. Click the  icon next to **Unique Resource Data**.

The Administration Manager displays the Unique Target Data Form, shown in *Figure 105* with default text and sample data. All text boxes can be edited. Data fields depend on the available connectors and targets.

Figure 105: Unique Target Data Form



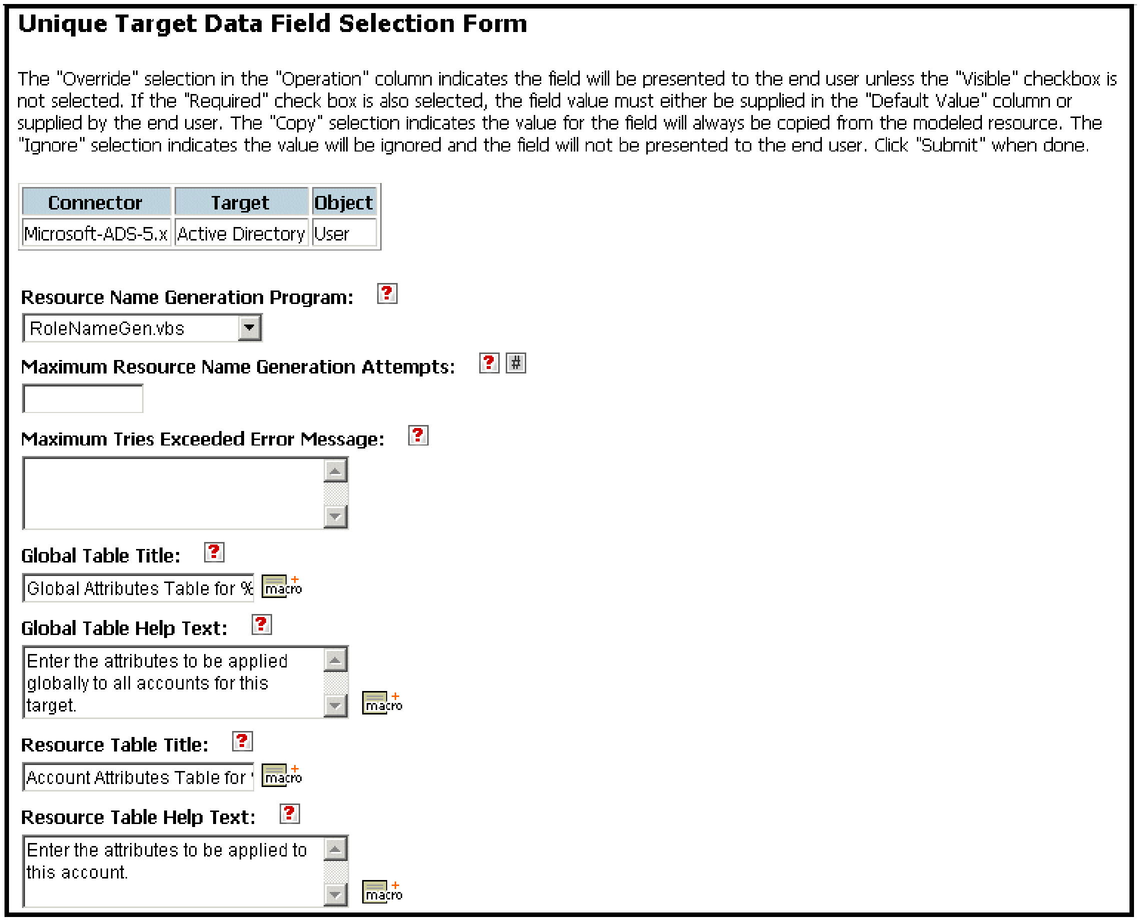
5. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
6. Text in the **Form Name** text box appears as a title on the form.
7. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)
8. Specify the file name or a macro that selects the **XSLT File for Processing**. This XSLT file is used for the presentation of data to the provisioner. It can be used to control which data is displayed and which is not, as well as how the data is formatted. It can also determine which kind of HTLML controls are rendered, controlling how provisioners interact with the data.

   To customize an XSLT file, copy the default file provided by Courion and rename it. Then edit the renamed file as needed and assign that file to this field.
9. In the **Dependency** column, select the name of the target where the first resource must be successfully provisioned before any other resources are provisioned.

   Note: In the Role Management sample workflow, the dependencies are configured serially, so the role record will not be created if any of the other accounts are unable to be provisioned. If you add any additional targets, Courion recommends that you maintain this configuration by chaining your new targets to be dependent on existing targets and then change the dependency of the Role Repository so that it is the final target in the chain.
10. In the **Configuration** column, click **Modify** to change the attribute settings for the Role Repository, Active Directory, or Exchange accounts. If you have added any additional targets, click **Create**.

The Administration Manager displays the Unique Target Data Field Selection Form. The actual content of this form depends on the connector. [Figure 106](#) shows the top of the form for the Connector for Microsoft Active Directory.

Figure 106: Unique Target Data Field Selection Form



11. RoleCourier can automatically generate a resource name on each selected target system.

    In the Role Management workflow, for the Microsoft Active Directory and Microsoft Exchange 2000 connectors, the RoleNameGen.vbs script is used to generate account names based on the role name. If you are adding targets to the workflow, assign this script to **RESOURCE NAME GENERATION PROGRAM** and then assign the appropriate macro to the account name attribute for the target. For more info, see *Table 5 on page 245*.

12. Text in the **GLOBAL TABLE TITLE** text box appears as the heading for the Global Attributes Table.

13. Text in the **GLOBAL TABLE HELP** Text text box appears as the help for the Global Attributes table.

14. Text in the **RESOURCE TABLE TITLE** text box appears as the heading for each Resource Attributes table.

15. Text in the **RESOURCE TABLE HELP TEXT** text box appears as the help for the Resource Attributes table.

16. Configure the attributes for the target. You can determine whether or not an attribute is exposed to the provisioner, whether it is required, whether the values may be mined from the Mining Community, etc. Up to twenty-five attributes for the selected target are displayed in a table. To view additional attributes, click the "next page" icon at the bottom of the table. For a description of all fields, see *Table 4 on page 77*.

    Some attributes allow for multiple values (in particular, the Group Membership attribute in Microsoft Active Directory). See *Table 5 on page 245* for more information.

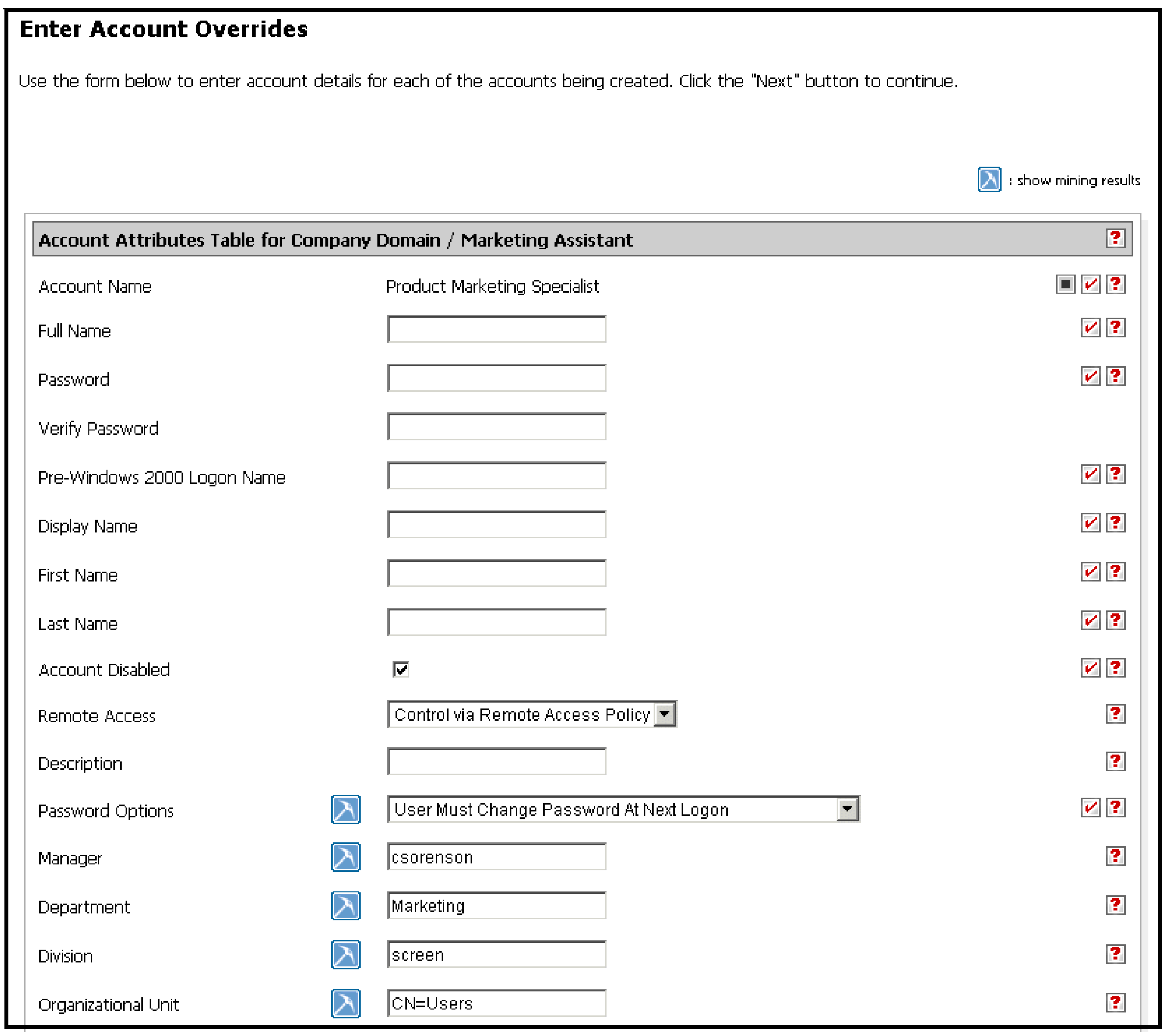
17. Click **Submit** after completing the Unique Target Data Field Selection Form.

    The Administration Manager redisplays the Unique Target Data Form (*Figure 105*).

18. Click **Create** or **Modify** for another connector to configure the set of attributes for another resource or click **Submit** to finish.

Figure 107 shows an example of part of the Enter Account Attributes screen displayed to the provisioner.

Figure 107: Enter Account Attributes for Role Screen

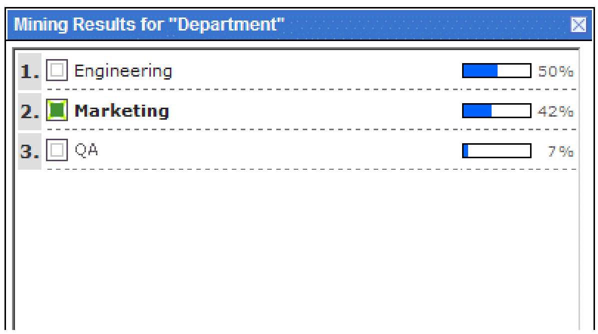


If the provisioner clicks on the Mining Icon, the Mining Results dialog box is displayed, as shown in *Figure 108*. (The Mining icon only appears if the **MINING** checkbox was selected in the **PRESENTATION** field on the Unique Target Data Field Selection Form.) The eight most common values for that attribute are displayed, along with the percentage of accounts within the Mining Community that contain the specific value. The value used by the baseline account is indicated by the green box.

Note: The percentage amounts of all the attribute values may not add up to 100%, due to the fact that percentage amounts are rounded down, and also because only the eight most common values are displayed.

Note: By default, the attribute values are case sensitive. So, for example, “Manager” will show up as a separate value from “manager”. If you want the attribute values to be case insensitive, change the **XSLT FILE FOR PROCESSING** field on the Unique Target Data Form from its default value of “ACCreateFormCtrls.xslt” to "CaseInsensitiveOverridesMining.xslt".

Figure 108: Mining Results



Change Account Attributes for an Existing Role

This section describes how to configure the Change action using the Courion Role Management sample workflow. This action enables a provisioner to change the attributes of the associated template accounts for existing roles.

With this workflow, a provisioner selects a role record that is stored in the transaction repository, and then edits the attributes of the template accounts associated with the role. The Role Management workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing role.
3. Use the Mining Community to select a group of users whose account access most closely matches the selected role.
4. Select the targets to edit, and then select the individual attributes and change the values as needed. For the attribute values, provisioners can view the values used by members of the mining community, helping them to select appropriate values for the template accounts.

The following sections describe configuration of the forms needed for the Change action:

- *"Configure Properties for the Change Resources Action" on page 216* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 218* describes how to set up a form the provisioner can complete to filter the role accounts available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 219* describes how to set up a form that displays the available role accounts. The provisioner selects the role for which they want to change attributes in template accounts.
- *"Refine the List of Displayed Mining Profiles" on page 223* describes how to set up a form that the user can complete to filter the mining profiles available in the workflow's community.
- *"Define a Mining Community" on page 224* describes how to set up a form that displays a table of users whose attributes can be "mined". The mined attributes are then displayed, enabling a provisioner to model attributes based on a group of users in stead of a single user.
- *"Define the IdentityMap Screen Presentation for the Change Action" on page 225* describes how to set up a form that controls the appearance of the Select Roles to Change form presented to the provisioner.
- *"Specify Unique Resource Data Fields for the Target" on page 226* describes how to set up a form the provisioner uses to change attribute values in the template accounts associated with a role.

Configure Properties for the Change Resources Action

To modify the Properties for Change Resources Action Form:

Flowchart View

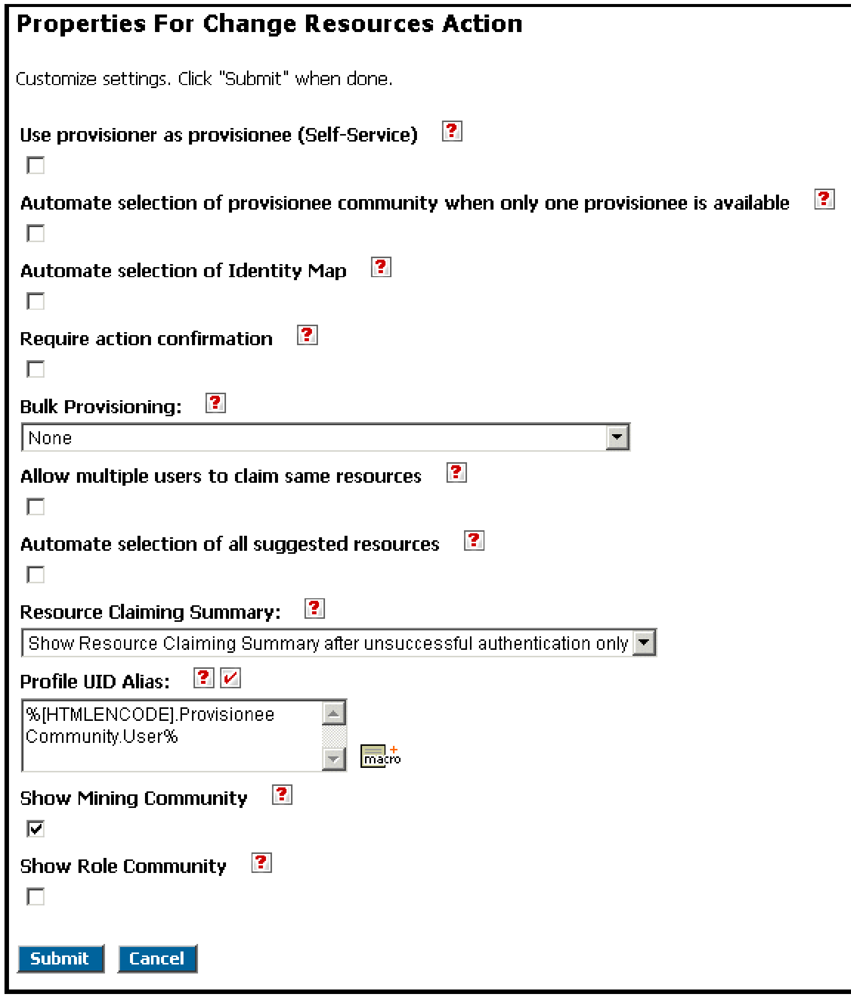
1. Log in to the Administration Manager Flowchart View.
2. Select **COURION ROLE MANAGEMENT** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CHANGE** from the **ACTION** drop-down menu.
4. Click on **CHANGE REQUEST**.
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS** and expand **CHANGE**.
4. Click the icon next to **PROPERTIES**.

   The Administration Manager displays the Properties for Change Resources Action Form, shown in *Figure 109*.

Figure 109: Properties for Change Resources Action Form



5. Leave the **Use provisioner as provisionee (Self-Service)** checkbox unchecked, since it does not apply in this workflow.

6. Select the **Automate selection of provisionee community when only one provisionee is available** checkbox to enable automatic selection of the provisionee profile (and to bypass the Provisionee Community screen) when only a single provisionee profile is retrieved from the connector. This setting is not selected by default.

   Since the “provisionee” is the role itself in the Role Management workflow, if this field is selected, it would be necessary to authenticate into the workflow using the role’s account name and password. Therefore it is likely you would not want to select this field.

7. Select the **Automate selection of IdentityMap** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **Submit** button. This setting is turned off by default.

8. Select the **Require action confirmation** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.

9. Leave the **Bulk Provisioning** option set to the default of None. This workflow does not use Bulk Provisioning.

10. Leave the **ALLOW MULTIPLE USERS TO CLAIM SAME RESOURCES** and **AUTOMATE SELECTION OF ALL SUGGESTED RESOURCES** checkboxes unchecked since this workflow does not use resource claiming.
11. Leave the **RESOURCE CLAIMING SUMMARY** option set to “Show Resource Claiming Summary after unsuccessful authentication only”.
12. The **PROFILE UID ALIAS** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the Courion Role Management sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
13. Leave the **SHOW MINING COMMUNITY** checkbox selected since this workflow uses the mining community.
14. Leave the **SHOW ROLE COMMUNITY** checkbox unselected since this workflow does not use the role community.
15. Click **SUBMIT**.

Refine the List of Displayed Provisionee Profiles

In the Change action of the Role Management workflow, the “provisionee” is the role itself.

By default, RoleCourier displays all the role records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of roles can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Role Search screen (*Figure 110*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of roles that meet the Provisionee Refine Search criteria. The provisioner then selects a role from the list for which account attributes are changed.

The provisioner can choose to skip entering data on the Role Search screen. If the screen is skipped, RoleCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Role Search screen is not displayed to the provisioner, by unchecking the **ACTIVE** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURION ROLE MANAGEMENT** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **CHANGE** from the navigation bar.
4. Click on **CHANGE REQUEST** and click on **PROVISIONEE REFINE SEARCH**.

Tree View

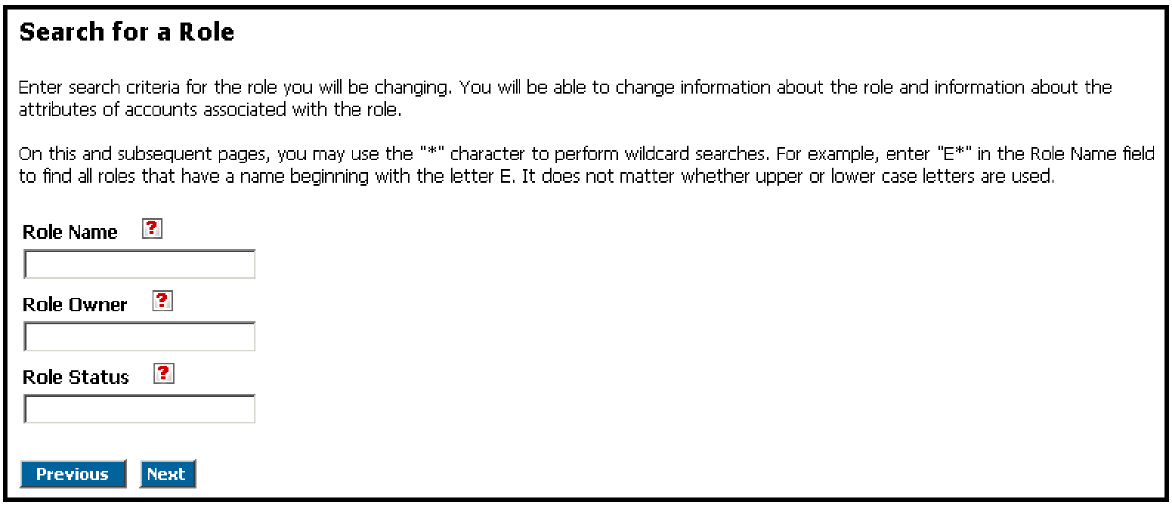
1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS** and expand **CHANGE**.
4. Click the  icon next to **PROVISIONEE REFINE SEARCH**.

The process to refine the list of displayed profiles from a Provisionee Community in the Change action of the Role Management workflow is the same as in any provisioning workflow. (The major difference is that instead of search for users, the provisioner is searching for roles. This is determined by the selection of the RoleCommunityView object in the transaction repository, which is configured on the Define Provisionee Community form.)

Refer to *Table 5 on page 245* for information on this form.

Figure 110 shows the screen displayed to provisioner, based on the settings from the Role Management workflow.

Figure 110: Role Search Screen



Define a Provisionee Community

In the Role Management workflow, the “provisionee” is the role itself. The Provisionee Community consists of the role records stored in the transaction repository.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the **Action** drop-down menu.
4. Click on **Change Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

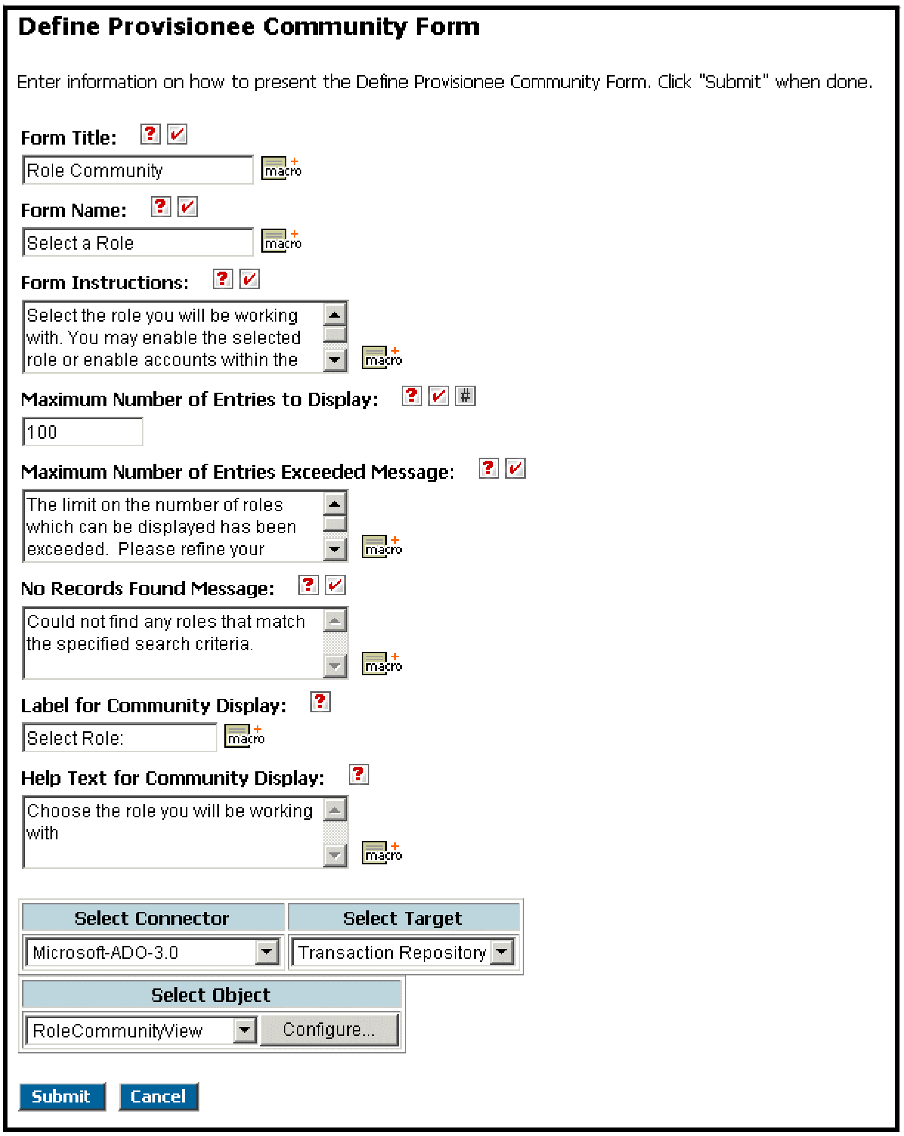
1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Provisionee Community**.

   The Administration Manager displays the Define Provisionee Community Form, shown in *Figure 111* with default text and sample data. You can edit all text boxes.

Figure 111: Define Provisionee Community Form



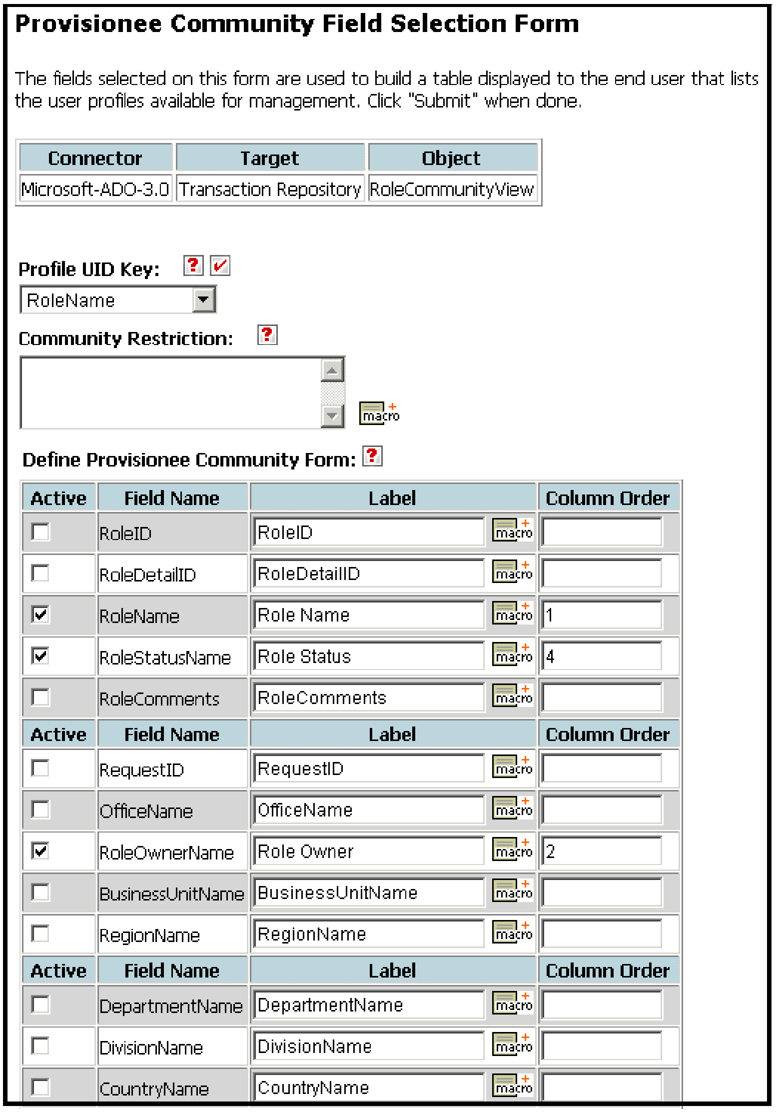
4. Text in the **Form Title** text box appears in the title bar of the Web Access Client browser window.
5. Text in the **Form Name** text box appears as a title on the form.
6. Text in the **Form Instructions** text box describes the purpose of the form. The text can be formatted using HTML. (For this reason, any text contained with the “<“ and “>” is considered an HTML tag and is not displayed.)

7. In the **Maximum Number of Entries to Display** text box, enter a number specifying the maximum number of profiles to display. If the filtering criteria for this form are broad or the company is large, the community defined by this form may be extensive. The value in this text box, combined with the Provisionee Refine Search Form, can help the provisioner limit the number of returned profiles (see *“Refine the List of Displayed Provisionee Profiles” on page 218*).
8. In the **Maximum Number of Entries Exceeded Message** text box, enter text warning the provisioner that the community includes more profiles but they cannot be listed because the **Maximum Number of Entries to Display** value has been reached. Advise the provisioner to use the Provisionee Refine Search Form to display profiles that more closely match search criteria.
9. In the **No Records Found Message** text box, enter text warning the provisioner that there are no profiles that match the search criteria. This message will display if the provisioner has entered values on the Provisionee Refine Search Form that do not match any profiles in the datasource. Advise the provisioner to reenter values on the Provisionee Refine Search Form or to skip the form to return a list of all profiles in the community.
10. Text in the **Label for Community Display** text box appears as a title over the Mining Community list.
11. Text in the **Help Text For Community Display** describes the action to take in the community display.
12. Leave the **Select Connector** drop-down list box set to Microsoft ADO, the **Select Target** drop-down list box set to Transaction repository, and the **Object** drop-down list box set to RoleCommunityView.
13. Click **Configure...**.

    The Administration Manager displays the Define Provisionee Community Field Selection Form, shown in *Figure 112*.

    Note: The list of fields has been shortened to save space.

Figure 112: Define Provisionee Community Field Selection Form



Provisionee Community Field Selection Form

The fields selected on this form are used to build a table displayed to the end user that lists the user profiles available for management. Click "Submit" when done.

Connector	Target	Object
Microsoft-ADO-3.0	Transaction Repository	RoleCommunityView

Profile UID Key:

RoleName

Community Restriction:

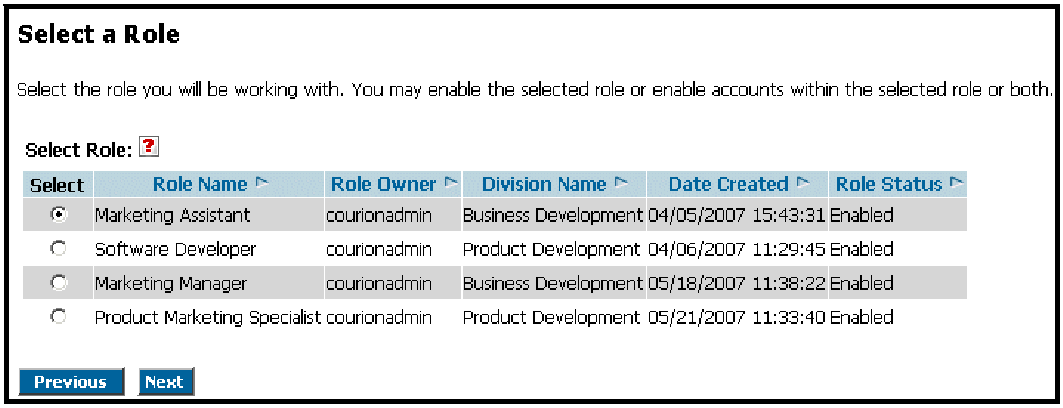
Define Provisionee Community Form:

Active	Field Name	Label	Column Order
☐	RoleID	RoleID	
☐	RoleDetailID	RoleDetailID	
☑	RoleName	Role Name	1
☑	RoleStatusName	Role Status	4
☐	RoleComments	RoleComments	
Active	**Field Name**	**Label**	**Column Order**
☐	RequestID	RequestID	
☐	OfficeName	OfficeName	
☑	RoleOwnerName	Role Owner	2
☐	BusinessUnitName	BusinessUnitName	
☐	RegionName	RegionName	
Active	**Field Name**	**Label**	**Column Order**
☐	DepartmentName	DepartmentName	
☐	DivisionName	DivisionName	
☐	CountryName	CountryName	

14. In the **ACTIVE** column, select the fields to use in the table displayed to the provisioner.
15. The **LABEL** column displays the field name by default. This text appears next to the associated field input box on the provisioner authentication form. You can edit these fields. For example, you could change "EmployeeBadgeNumber" field to "Badge number:".
16. The **HELP TEXT** column includes default help text for each field name. This text appears when the provisioner hovers the mouse pointer over the help icon for the field on the form. You can edit these fields. You can also use the Macro button to customize the displayed help text.
17. In the **COLUMN ORDER** column, enter a number for each selected field to determine the order the field names appear as column headers. The field numbered "1" appears as the first column.
18. Click **SUBMIT**.

Figure 113 shows the screen displayed to provisioner, based on the settings from the example above.

Figure 113: Select Role Screen



Refine the List of Displayed Mining Profiles

The Courion Role Management sample workflow uses the Mining Community to select a group of roles whose account access most closely matches the role whose attributes you want to edit.

By default, RoleCourier displays all the roles to the provisioner that meet the criteria configured in the Define Mining Community Form. If the filtering criteria for the Define Mining Community Form are broad or the company is large, the community of roles can be extensive. You can select one or more fields to include on a Mining Refine Search Form. These fields are presented to the provisioner. The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of roles that meet the Mining Refine Search criteria. The provisioner then selects one or more roles to be used for mining.

The provisioner can choose to skip entering data on this form. If the form is skipped, RoleCourier returns all the user profiles established by the Define Mining Community Form.

To modify the Mining Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the **Action** drop-down menu.
4. Click on **Change Request**.
5. Click on **Mining Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Change**.
4. Click the  icon next to **Mining Refine Search**.

The process to refine the list of displayed profiles from a Mining Community in the Change Action of the Role Management workflow is the same as for a Create Action in any provisioning workflow.

Refer to *Table 5 on page 245* for information on this form.

Define a Mining Community

The Mining Community is a set of existing entities in a database or directory whose attributes may be used as a model for selecting attributes for an account that is being provisioned. Although in many cases the Mining Community consists of users, in the case of the role Management workflow, the Mining Community consists of other roles.

Note: The Mining Community is global and affects all actions within a workflow. Therefore, any changes made will apply to all the actions in the Role Management workflow.

Note: For the Mining Community to be displayed to the provisioner, the **Show Mining Community** on the Properties form must be selected. (This field is selected by default in the Role Management workflow.)

Note: To use the Mining functionality, at least one attribute must have the **Mining** option selected in the **Presentation** field on the Unique Target Data Field Selection Form. See *"Specify Unique Resource Data Fields for the Target" on page 210* for details.

To modify the Define Mining Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the **Action** drop-down menu.
4. Click on **Change Request**.
5. Click on **Mining Community**.

   Note: You can also access the Mining Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Mining Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Mining Community**.

The process to configure the Mining Community for a Change Action is the same as for a Create Action.

To modify the Mining Community Form and the forms that follow, complete the steps described in *"Define a Mining Community" on page 195*.

Define the IdentityMap Screen Presentation for the Change Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Change screen, shown in *Figure 114*.

Note: If the **Automate selection of IdentityMap** on the Properties form is enabled, this form is skipped in the workflow, all of the role's template accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter Role and Account Information screen to the provisioner).

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the navigation bar.
4. Click on **Change Request** and click on **IdentityMap Screen**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions**, expand **Change**, expand **Action Settings**, and click the icon next to **IdentityMap Screen**.

The process to modify the fields for the IdentityMap Screen in the Change action of the Role Management workflow is the same as for a Change action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

In the Courion Role Management sample workflow there are two tabs, labelled "Corporate Systems" and "Role Management". The labels for these tabs are determined by the values chosen in the **Category** field found on the Add and Modify Target forms. Targets configured with the same category name will show up under a single tab. If no category is specified, the target will show up under a tab labelled "Accounts". (For more details on configuring targets, see *Table 5 on page 245*.)

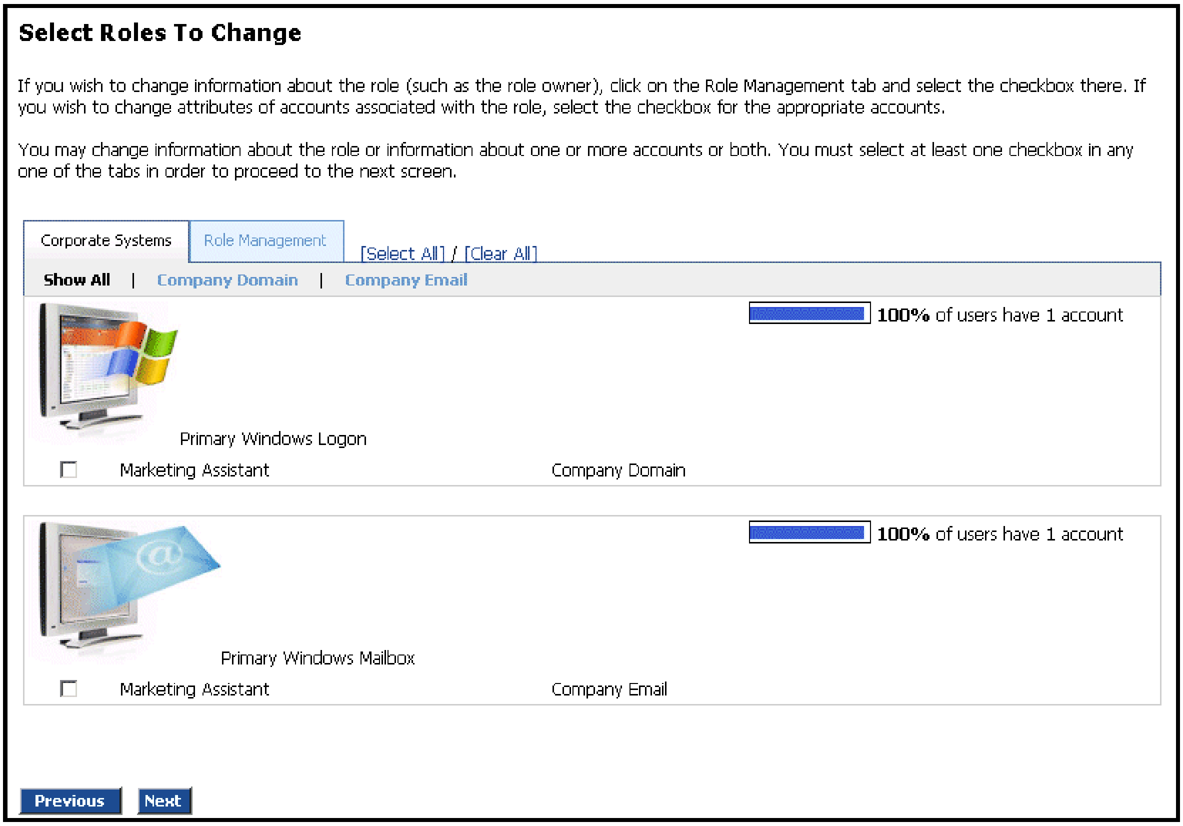
In the case of the sample workflow, the Courion Role Connector has been given its own separate category to help distinguish that this target is used for maintenance of the role itself, whereas the other targets are used to create template accounts that link to the role.

The names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. If one or more users have been selected from the mining community, both a resource description and a popularity indicator are displayed above the resource name, checkbox, and target name. The description is taken from the **Description** field on the Add and Modify Target forms. If no mining users are selected, only the resource name, checkbox, and target name are displayed. As shown in *Figure 114*, the description can include a graphic.

In the Change action of the Role Management workflow, the Role Management target is selected automatically and may not be unselected. This is determined by the RoleSampleIDMap.xslt file assigned in the **XSLT File for Processing** field. The attributes of the role itself are displayed for reference on the following screen. They may be edited, or left as is.

Figure 114: Select Accounts to Change Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are displayed to the provisioner. The Courion Role Management sample workflow has three targets already configured - the Role Repository (for creation of the role itself), Active Directory (for a logon ID), and Microsoft Exchange (for an email account). If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. See *Table 5 on page 245* for details.

Once a target is available, you click on Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which will display mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Change** from the **Action** drop-down menu.
4. Click on **Change Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.

2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS** and expand **CHANGE**.
4. Click the icon next to **UNIQUE RESOURCE DATA**.

The steps to complete the Unique Target Data Form to change a resource are the same as to create a resource. Follow the instructions provided in *"Specify Unique Resource Data Fields for the Target" on page 210*.

Disabling and Enabling a Role and its Template Accounts

This section describes how to configure the Disable and Enable actions using the Courion Role Management sample workflow. These actions enable a provisioner to disable and enable a role and its associated template accounts.

With this workflow, a provisioner selects a role record that is stored in the transaction repository, and then disables or enables the role or its associated template accounts or both. The Role Management workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing role.
3. Select the targets to disable or enable.
4. If the provisioner selects the role itself, he or she can enter a comment regarding the enabling or disabling of the role. In addition, when enabling a Microsoft Exchange Mailbox account, the number of recipients must be specified. (The exposure of both the comment and number of recipients is determined by the configuration of the Unique Target Data form for the respective targets and may therefore be changed. See *“Specify Unique Resource Data Fields for the Target” on page 210* for details.)

The steps to configure the forms for the Disable and Enable actions are virtually identical. Therefore, while the following descriptions of each form refers to the Disable action, they also apply to the Enable action.

The following sections describe configuration of the forms needed for the Disable and Enable actions:

- *“Configure Properties for the Disable Resources Action” on page 229* determines which forms are presented to the provisioner.
- *“Refine the List of Displayed Provisionee Profiles” on page 231* describes how to set up a form the provisioner can complete to filter the role accounts available in the workflow’s provisionee community.
- *“Define a Provisionee Community” on page 232* describes how to set up a form that displays the available role accounts. The provisioner selects the role for which they want to disable roles or template accounts.
- *“Define the IdentityMap Screen Presentation for the Disable Action” on page 233* describes how to set up a form that controls the appearance of the Select Accounts/Roles to Disable form presented to the provisioner.
- *“Specify Unique Resource Data Fields for the Target” on page 234* describes how to set up a form the provisioner completes that specifies the fields and possible default values used when disabling a role or template account.

Configure Properties for the Disable Resources Action

To modify the Properties for Disable Resources Action Form:

Flowchart View

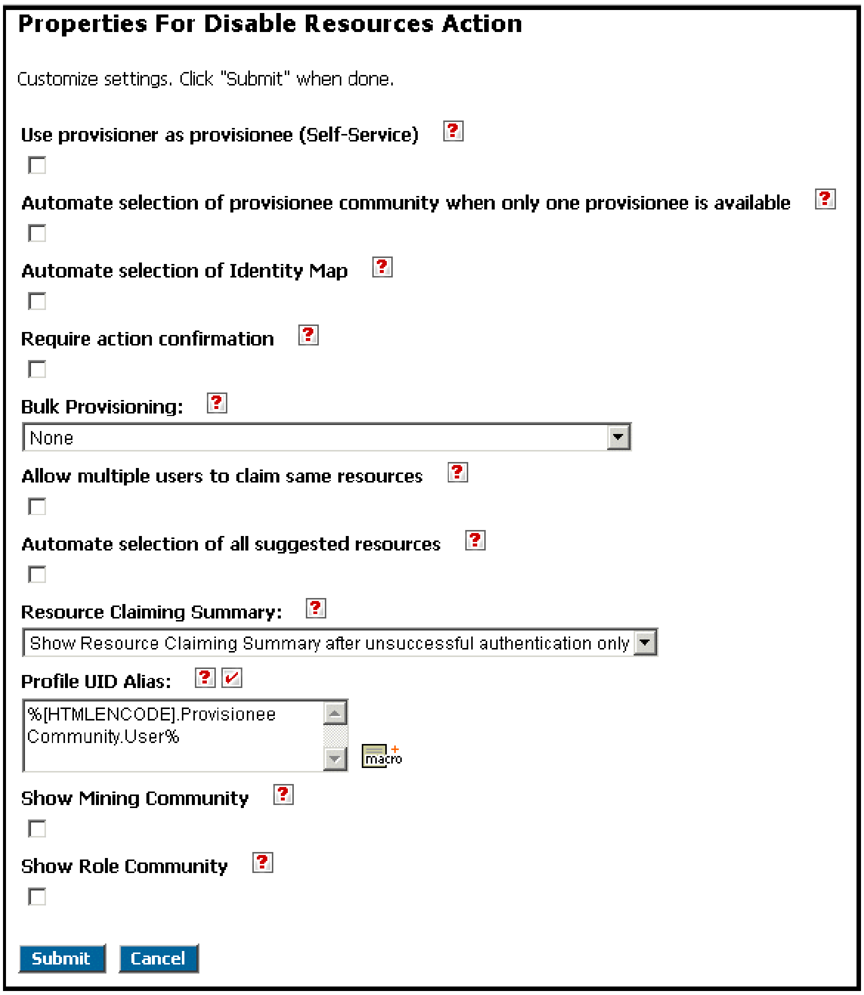
1. Log in to the Administration Manager Flowchart View.
2. Select **COURION ROLE MANAGEMENT** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **DISABLE** from the **ACTION** drop-down menu.
4. Click on **DISABLE REQUEST**.
5. Click on **PROPERTIES**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS** and expand **DISABLE**.
4. Click the icon next to **PROPERTIES**.

   The Administration Manager displays the Properties for Disable Resources Action Form, shown in *Figure 115*.

Figure 115: Properties for Disable Resources Action Form



5. Leave the **Use provisioner as provisionee (Self-Service)** checkbox unchecked, since it does not apply in this workflow.

6. Select the **Automate selection of provisionee community when only one provisionee is available** checkbox to enable automatic selection of the provisionee profile (and to bypass the Provisionee Community screen) when only a single provisionee profile is retrieved from the connector. This setting is not selected by default.

   Since the "provisionee" is the role itself in the Role Management workflow, if this field is selected, it would be necessary to authenticate into the workflow using the role's account name and password. Therefore it is likely you would not want to select this field.

7. Select the **Automate selection of IdentityMap** checkbox to enable automatic selection of all targets (and bypass the IdentityMap screen). This is the same behavior that would occur if a provisioner selected all targets on the IdentityMap screen and clicked the **Submit** button. This setting is turned off by default.

8. Select the **Require action confirmation** checkbox to have the workflow prompt the provisioner with a confirmation form. This setting is turned off by default. If you do not select this option, the confirmation form does not appear and the workflow skips this step.

9. Leave the **Bulk Provisioning** option set to the default of None. This workflow does not use Bulk Provisioning.

10. Leave the **Allow multiple users to claim same resources** and **Automate selection of all suggested resources** checkboxes unchecked since this workflow does not use resource claiming.
11. Leave the **Resource Claiming Summary** option set to “Show Resource Claiming Summary after unsuccessful authentication only”.
12. The **Profile UID Alias** represents the profile UID in a user-friendly way. For example, you could use a custom macro that resolved an employee badge number to an employee name. In the Courion Role Management sample workflow, this is set to %[HTMLENCODE].Provisionee Community.User%.
13. Leave the **Show Mining Community** checkbox unselected since this workflow does not use the mining community.
14. Leave the **Show Role Community** checkbox unselected since this workflow does not use the role community.
15. Click **Submit**.

Refine the List of Displayed Provisionee Profiles

In the Disable action of the Role Management workflow, the “provisionee” is the role itself.

By default, RoleCourier displays all the role records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of roles can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Role Search screen (*Figure 110*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of roles that meet the Provisionee Refine Search criteria. The provisioner then selects a role from the list for which account attributes are changed.

The provisioner can choose to skip entering data on the Role Search screen. If the screen is skipped, RoleCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Role Search screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Disable** from the navigation bar.
4. Click on **Disable Request** and click on **Provisionee Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Disable**.
4. Click the icon next to **Provisionee Refine Search**.

The process to refine the list of displayed profiles from a Provisionee Community in the Disable action of the Role Management workflow is the same as in any provisioning workflow. (The major difference is that instead of search for users, the provisioner is searching for roles. This is determined by the selection of the RoleCommunityView object in the transaction repository, which is configured on the Define Provisionee Community form.)

Refer to *Table 5 on page 245* for information on this form.

Define a Provisionee Community

In the Role Management workflow, the “provisionee” is the role itself. The Provisionee Community consists of the role records stored in the transaction repository.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Disable** from the **Action** drop-down menu.
4. Click on **Disable Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

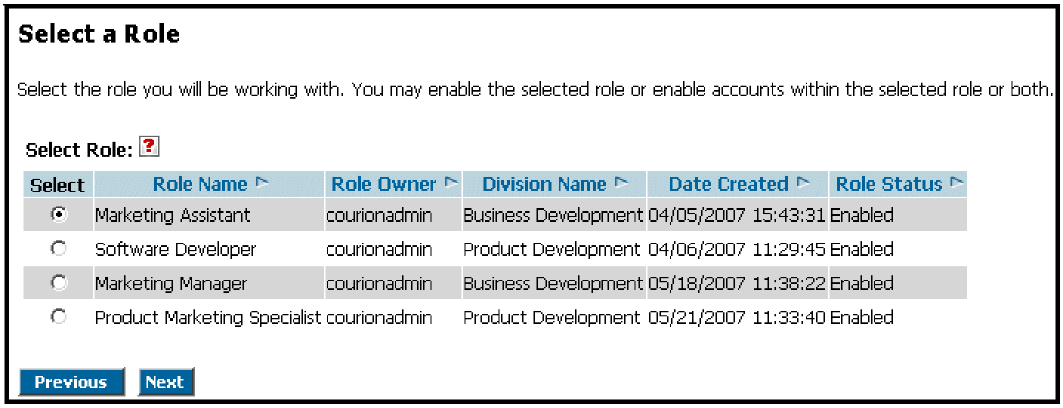
Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Provisionee Community**.

   The process to define the Provisionee Community in the Disable action of the Role Management workflow is the same as in the Change action. See *“Define a Provisionee Community” on page 219* for information about how to complete this form.

Figure 116 shows the screen displayed to provisioner.

Figure 116: Select Role Screen



Define the IdentityMap Screen Presentation for the Disable Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Disable screen, shown in *Figure 117*.

Note: If the **AUTOMATE SELECTION OF IDENTITYMAP** on the Properties form is enabled, this form is skipped in the workflow, all of the user's accounts are selected, and the workflow proceeds to the Unique Resource Data form (used to display the Enter Comment screen to the provisioner).

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **COURION ROLE MANAGEMENT** from the **WORKFLOW** drop-down menu.
3. Select **BUSINESS PROCESS** and **DISABLE** from the navigation bar.
4. Click on **DISABLE REQUEST** and click on **IDENTITYMAP SCREEN**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **COURION ROLE MANAGEMENT** workflow.
3. Expand **ACTIONS**, expand **DISABLE**, expand **ACTION SETTINGS**, and click the icon next to **IDENTITYMAP SCREEN**.

The process to modify the fields for the IdentityMap Screen in the Disable action of the Role Management workflow is the same as for a Change action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

In the Courion Role Management sample workflow there are two tabs, labelled "Corporate Systems" and "Role Management". The labels for these tabs are determined by the values chosen in the **CATEGORY** field found on the Add and Modify Target forms. Targets configured with the same category name will show up under a single tab. If no category is specified, the target will show up under a tab labelled "Accounts". (For more details on configuring targets, see *Table 5 on page 245*.)

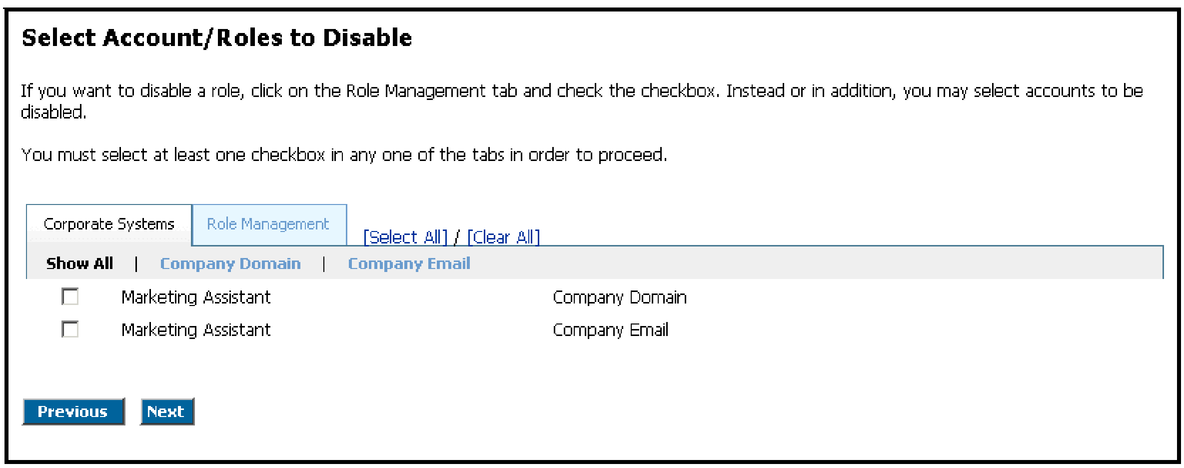
In the case of the sample workflow, the Courion Role Connector has been given its own separate category to help distinguish that this target is used for maintenance of the role itself, whereas the other targets are used to create template accounts that link to the role.

The names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. If one or more users have been selected from the mining community, both a resource description and a popularity indicator are displayed above the resource name, checkbox, and target name. The description is taken from the **Description** field on the Add and Modify Target forms. If no mining users are selected, only the resource name, checkbox, and target name are displayed.

Note: In the Disable action of the Role Management workflow, the Role Repository target is selected automatically and may not be unselected. This is determined by the RoleSampleIDMap.xslt file assigned in the **XSLT File for Processing** field. For this reason, it is not possible for the provisioner to disable one or more of the template accounts without also disabling the role itself. However, you can change the workflow so that the provisioner can choose whether or not to select the Role Repository target, by changing the value of the **XSLT File for Processing** field to ACCreateFormCtrls.xslt

Figure 117: Select Accounts to Disable Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are displayed to the provisioner. For the purpose of disabling or enabling an account, it is not necessary to expose any attributes. However, depending on the target and the available attributes, it can be useful to expose certain attributes. The Courion Role Management sample workflow has two targets configured to display attributes. The Role Repository target displays the Comments and Role Owner, enabling the provisioner to provide documentation on the reason for the disabling or enabling. The Microsoft Exchange displays the Number of Recipients field on the Enable action only, requiring the provisioner to enter a number when the account is enabled.

The Active Directory target can be disabled or enabled in the Role Management workflow, but no attributes are exposed by default.

If you need to add additional targets, they must first be configured on the Target Configuration form found in the global settings. See *Table 5 on page 245* for details.

Once a target is available, you click on Create or Modify to access the individual attributes for that target and determine which are exposed to the provisioner, which will display mining data, etc.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Disable** from the **Action** drop-down menu.
4. Click on **Disable Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Disable**.
4. Click the  icon next to **Unique Resource Data**.

The steps to complete the Unique Target Data Form to Disable a resource are the same as to create a resource. Follow the instructions provided in *"Specify Unique Resource Data Fields for the Target" on page 210*.

Deleting the Template Accounts for a Role

This section describes how to configure the Delete action using the Courion Role Management sample workflow. This action enables a provisioner to delete the template accounts associated with a role. The role itself can not be deleted.

With this workflow, a provisioner selects a role record that is stored in the transaction repository, and then chooses which of its associated template accounts to delete. The Role Management workflow enables provisioners to:

1. Authenticate into the workflow using their Active Directory account name and password.
2. Select an existing role.
3. Select the targets to delete.

The following sections describe configuration of the forms needed for the Delete action:

- *"Configure Properties for the Delete Resources Action" on page 236* determines which forms are presented to the provisioner.
- *"Refine the List of Displayed Provisionee Profiles" on page 237* describes how to set up a form the provisioner can complete to filter the role accounts available in the workflow's provisionee community.
- *"Define a Provisionee Community" on page 238* describes how to set up a form that displays the available role accounts. The provisioner selects the role or which they want to delete template accounts.
- *"Define the IdentityMap Screen Presentation for the Delete Action" on page 238* describes how to set up a form that controls the appearance of the Select Accounts to Delete form presented to the provisioner.
- *"Specify Unique Resource Data Fields for the Target" on page 240* describes how to set up a form the provisioner completes that specifies the fields and possible default values used when deleting a template account.

Configure Properties for the Delete Resources Action

To modify the Properties for Delete Action Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the **Action** drop-down menu.
4. Click on **Delete Request**.
5. Click on **Properties**.

Tree View

1. Log in to the Administration Manager Tree View.

2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Delete**.
4. Click the icon next to **Properties**.

The steps to set up a Properties Form for the Delete action of the Role Management workflow is the same as for the Disable action in this workflow. Follow the instructions provided in *"Configure Properties for the Disable Resources Action" on page 229*

Refine the List of Displayed Provisionee Profiles

In the Delete action of the Role Management workflow, the "provisionee" is the role itself.

By default, RoleCourier displays all the role records to the provisioner that meet the criteria configured in the Define Provisionee Community Form. If the filtering criteria for the Define Provisionee Community Form are broad or the company is large, the number of roles can be extensive. You can select one or more fields to include on a Provisionee Refine Search Form. These fields are presented to the provisioner on the Role Search screen (*Figure 110*). The provisioner enters values for one or more fields and RoleCourier searches the community and returns a list of roles that meet the Provisionee Refine Search criteria. The provisioner then selects a role from the list for which account attributes are changed.

The provisioner can choose to skip entering data on the Role Search screen. If the screen is skipped, RoleCourier returns all the user profiles established by the Define Provisionee Community Form. You may also configure Provisionee Refine Search Form so that the Role Search screen is not displayed to the provisioner, by unchecking the **Active** checkbox for all search fields.

To modify the Provisionee Refine Search Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the navigation bar.
4. Click on **Delete Request** and click on **Provisionee Refine Search**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Delete**.
4. Click the icon next to **Provisionee Refine Search**.

The process to refine the list of displayed profiles from a Provisionee Community in the Delete action of the Role Management workflow is the same as in any provisioning workflow. (The major difference is that instead of search for users, the provisioner is searching for roles. This is determined by the selection of the RoleCommunityView object in the transaction repository, which is configured on the Define Provisionee Community form.)

Refer to *Table 5 on page 245* for information on this form.

Define a Provisionee Community

In the Role Management workflow, the “provisionee” is the role itself. The Provisionee Community consists of the role records stored in the transaction repository.

To modify the Define Provisionee Community Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the **Action** drop-down menu.
4. Click on **Delete Request**.
5. Click on **Provisionee Community**.

   Note: You can also access the Provisionee Community form in Flowchart View using this method:

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Click on **Dynamic Communities** from the navigation bar.
4. Click on **Provisionee Community**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions**, expand **Global Settings**, and click the icon next to **Provisionee Community**.

   The process to define the Provisionee Community in the Delete action of the Role Management workflow is the same as in the Change action. See *“Define a Provisionee Community” on page 219* for information about how to complete this form.

Define the IdentityMap Screen Presentation for the Delete Action

The IdentityMap Screen form controls the labels and formatting for the Select Accounts to Delete screen, shown in *Figure 118*.

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the navigation bar.
4. Click on **Delete Request** and click on **IdentityMap Screen**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions**, expand **Delete**, expand **Action Settings**, and click the icon next to **IdentityMap Screen**.

The process to modify the fields for the IdentityMap Screen in the Delete action of the Role Management workflow is the same as for a Change action in any provisioning workflow. Refer to *Table 5 on page 245* for information on this form.

In the Courion Role Management sample workflow there are two tabs, labelled “Corporate Systems” and “Role Management”. The labels for these tabs are determined by the values chosen in the **Category** field found on the Add and Modify Target forms. Targets configured with the same category name will show up under a single tab. If no category is specified, the target will show up under a tab labelled “Accounts”. (For more details on configuring targets, see *Table 5 on page 245*.)

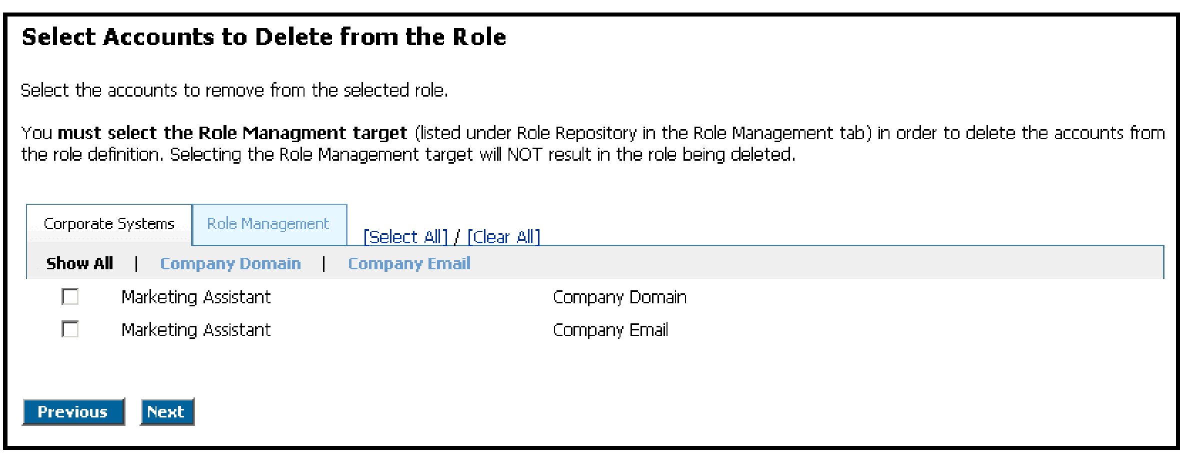
In the case of the sample workflow, the Courion Role Connector has been given its own separate category to help distinguish that this target is used for maintenance of the role itself, whereas the other targets are used to create template accounts that link to the role.

The names of the individual targets in the grey menu bar are taken from the **Alias** field on the Add and Modify Target forms. If no alias is specified, the **IdentityMap Target ID** field is used.

A list of accounts belonging to the model account appears below the grey menu bar. If one or more users have been selected from the mining community, both a resource description and a popularity indicator are displayed above the resource name, checkbox, and target name. The description is taken from the **Description** field on the Add and Modify Target forms. If no mining users are selected, only the resource name, checkbox, and target name are displayed.

Note: In the Delete action of the Role Management workflow, the Role Management target is selected automatically and may not be unselected. This is determined by the RoleSampleIDMap.xslt file assigned in the **XSLT File for Processing** field. The Role record in the transaction repository is **not** deleted, but it needs to be selected so that the role definition is changed to reflect the correct status of which template accounts are associated with the role.

Figure 118: Select Accounts to Delete Screen



Specify Unique Resource Data Fields for the Target

You use the Unique Target Data form to configure which attributes are displayed to the provisioner. For the purpose of deleting an account, most targets do not expose any attributes. However, the Role target does enable you to expose attributes. In the Role Management sample workflow, the Comments attribute is displayed, enabling the provisioner to provide comments regarding the deletion of template accounts.

To modify the Unique Target Data Form:

Flowchart View

1. Log in to the Administration Manager Flowchart View.
2. Select **Courion Role Management** from the **Workflow** drop-down menu.
3. Select **Business Process** and **Delete** from the **Action** drop-down menu.
4. Click on **Delete Request**.
5. Click on **Unique Resource Data**.

Tree View

1. Log in to the Administration Manager Tree View.
2. Expand the **Courion Role Management** workflow.
3. Expand **Actions** and expand **Delete**.
4. Click the  icon next to **Unique Resource Data**.

Click on Modify for the Role Repository to access the individual attributes and determine which are exposed to the provisioner.

The steps to complete the Unique Target Data Form to Delete a resource are the same as to create a resource. Follow the instructions provided in *“Specify Unique Resource Data Fields for the Target” on page 210*.

Appendix A: Copying Sample Workflows

Core Security strongly recommends that if you want to edit the Administration Manager forms for a sample workflow, that you create a new workflow by copying the one you want to edit. You can then edit the new workflow while maintaining the original workflow for reference. Another reason for creating a new workflow is that if you reinstall the Access Assurance Suite for some reason or upgrade to a higher version, you can overwrite the preconfigured workflows, including the sample workflows. In this situation, you would lose any edits you made to the sample workflow.

Creating a Workflow by Copying an Existing Workflow

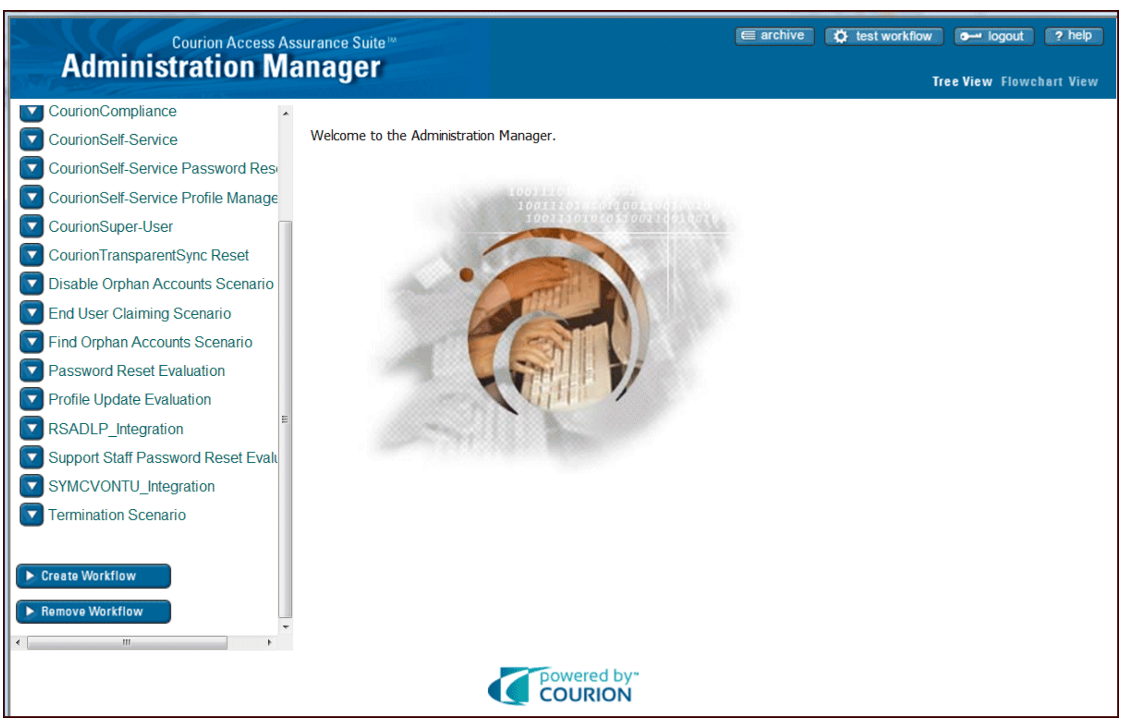
Follow these steps to create a workflow by copying an existing workflow in Tree View or Flowchart View:

1. From the Administration Manager, select the Create Workflow option in Tree View or Flowchart View.

   To create a workflow in Tree View:

   Click the Create Workflow button under the list of workflows, as shown in *Figure 119*.

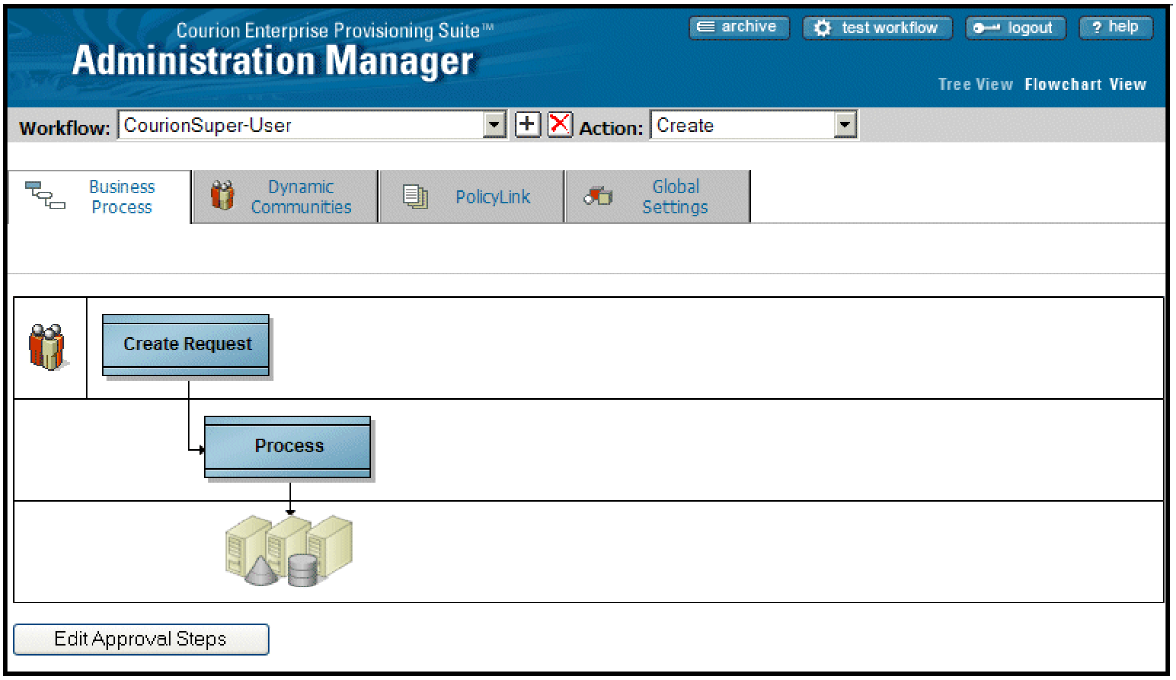
Figure 119: Workflow List in Tree View



   To create a workflow in Flowchart View:

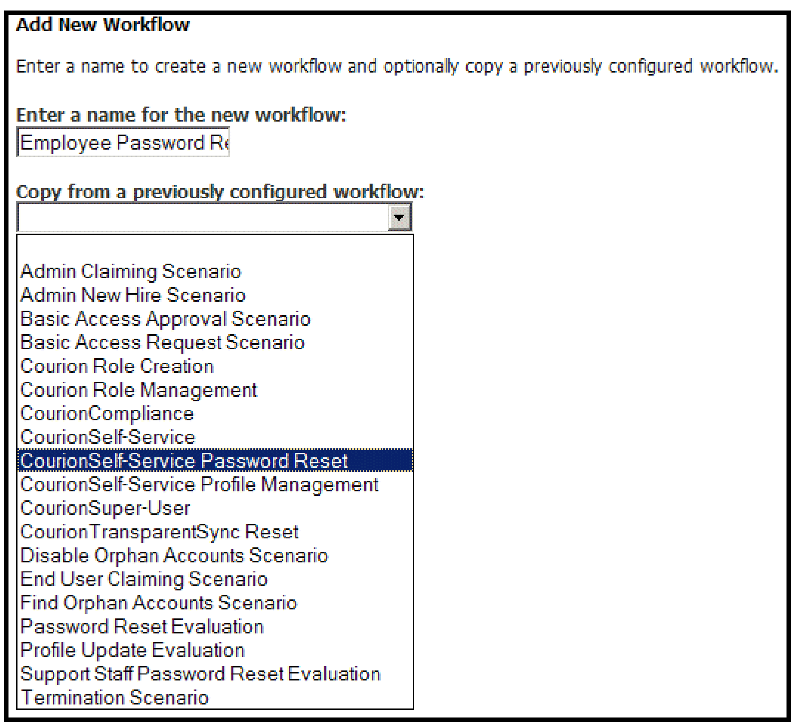
   Click the plus sign (**+**) next to the workflow name, as shown in *Figure 120*.

Figure 120: Sample Workflow in Flowchart View'



2. Enter the name of the new workflow, as shown in *Figure 121*.

Figure 121: Enter New Workflow Name



For example, if you wanted to create a workflow similar to CourionSelf-Service Password Reset, you could name it Employee Password Reset.

Note: Do not use the following characters when naming a workflow: # (pound sign), % (percent), & (ampersand), ' (single quote), < (left angle bracket). The # (pound sign), % (percent), and & (ampersand) characters will not resolve properly when entered as part of a URL in your browser's Address bar. The ' (single quote) and < (left angle bracket) will generate unusable workflows.

3. Select another workflow from the **COPY FROM AN PREVIOUSLY CONFIGURED WORKFLOW** drop-down list. In this example, you would select CourionSelf-Service Password Reset.

   Note: In Flowchart View, it does not matter which workflow is selected as the current workflow when you click the plus sign button—you can copy any existing workflow to the new workflow.

4. Click the **CREATE** button.

5. The new workflow now appears on the list of existing workflows and you can edit it in Tree View or Flowchart View.

Appendix B: References to Administration Manager Forms

To focus on the specific functionality of the various sample workflows, only the forms in which the configuration is significant to the functionality are discussed in detail in this manual. The other forms used in the workflows are described in detail in the manual *Configuring Workflows with the Access Assurance Suite Administration Manager*.

The following table provides reference information on the specific sections of that manual for the forms not discussed in detail here.

Table 5: Details on Forms and Functionality Not Described in this Manual

Form/Function	Chapter	Section
Action Group Configuration	Configure Global Actions and Settings	Configure Action Groups
Automatic Name Creation	Configuring Provisioning Workflows	Set Up the Resource Create Action
Authentication	Setting Up Workflow Authentication	Create the Authentication Forms
Community Restriction parameter (found on all Community Field Selection forms)	Configure Global Actions and Settings	Define a Resource Community to Manager
Conditions	Creating Conditions	
Confirmation	Configuring Provisioning Workflows	Set Up the Resource Create Action
Functions (Password Strength for the Password Reset action)	Configuring Functions	Password Strength
IdentityMap	Configure Global Actions and Settings	Set Up the IdentityMap
IdentityMap Screen (for an Add action)	Configuring Provisioning Workflows	Set Up the Resource Add Action
IdentityMap Screen (for all other actions)	Configuring Provisioning Workflows	Set Up the Resource Create Action
Macros	Using Macros in a Workflow	
Mining Refine Search	Configuring Provisioning Workflows	Set Up the Resource Create Action

Table 5: Details on Forms and Functionality Not Described in this Manual

Form/Function	Chapter	Section
Multi-Value Attributes (Group Membership)	Configuring Provisioning Workflows	Set Up the Resource Create Action
Notification	Configuring Triggers, Tickets, and Notification	Setting Up Notification for an Event
Password Synchronization	Configuring Password Reset Workflows	Set Up the Password Reset Action
Provisionee Refine Search	Configuring Provisioning Workflows	Set Up the Resource Add Action
Resource Refine Search	Configuring Provisioning Workflows	Set Up the Resource Create Action
Sub-Worksheets (used in Compliance workflows)	Configure Global Actions and Settings also Configuring Compliance Workflows	Define Sub-Worksheets Configuring Conditions for Sub-worksheets in Compliance Workflows
Summary	Configuring Provisioning Workflows	Set Up the Resource Create Action
Target Configuration	Configure Global Actions and Settings	Target Configuration Form
Ticketing	Configuring Triggers, Tickets, and Notification	Setting Up Ticketing for an Event
Transaction Repository	Configure Global Actions and Settings	Activate a Transaction Repository
Triggers	Configuring Triggers, Tickets, and Notification	Setting Up a Trigger Configuration for an Event

INDEX

R

S

U

V

W