RSA Identity Management and Governance

Access Request Manager Guide
V6.9

Notice

Contact Information

Go to the RSA corporate website for regional Customer Support telephone and fax numbers: **www.emc.com/domains/rsa/index.htm**. For sales information, contact RSA Aveksa, Inc. at sales@aveksa.com For technical support, contact RSA Aveksa, Inc. at support@aveksa.com. For more information about RSA Aveksa, Inc., visit **http://www.aveksa.com**.

Trademarks

RSA, the RSA Logo, Aveksa, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed by launching the RSA Aveksa product and selecting the About menu.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

July 2014

Contents

Preface

Audience

This guide is intended for RSA Identity Management and Governance (RSA IMG) administrators authorized to manage Access Request Manager features and all users who want to leverage Access Request Manager to request access to entitlements and request changes to access.

For more information on change requests and request workflow features, see the following in the *Administrators Guide*:

- Chapter 18, "Working with Change Requests," on page 233
- Chapter 19, "Managing Change Request Workflows," on page 247

Note: *You require an Access Request Manager license to use Access Request Manager. Contact an RSA sales representative for more information.*

How This Guide Is Organized

This guide is organized as follows:

- Chapter 1, "Introduction," on page 11 describes Access Request Manager features and concepts.
- Chapter 2, "Specifying Access Request Configuration Settings," on page 17 describes how to configure Access Request Manager settings.
- Chapter 3, "Creating and Managing Access Request Buttons," on page 21 describes how to create and manage access request buttons on the user interface.
- Chapter 4, "Creating and Managing Access Request Forms," on page 27 describes how to create and manage custom access request forms.
- Chapter 5, "Creating Managing Access Request Views," on page 41 describes how to configure *v*iews of users and entitlements available to requestors when they request or change access.
- Chapter 6, "Creating and Managing Account Templates," on page 49 describes how to configure account templates that define how accounts should be created for applications and directories.

- Chapter 7, "Customizing Request Submission Forms," on page 55 describes how to configure additional action options that requestors must or can act upon when they submit a change request.
- Chapter 8, "Creating and Managing Change Request Activity Monitoring Policies," on page 65 describes how to create and manage monitoring policies that specify views of change request approvals and fulfillment activities available to particular sets of users.
- Chapter 9, "Managing Account Password Reset Implementation," on page 69 describes how to create and manage the password policies that specify the quality standards for user account password reset requests and how to configure challenge (or security) question standards for non-AveksaAdmin account login password resets.
- Chapter 10, "Set Up the System for New User Registration Requests," on page 81 describes how to set up requisite components in the system to support user registration (new user on-boarding) requests.
- Chapter 11, "Managing How Entitlements Are Requested Using Resource Profiles," on page 95 describes how to manage access to business source entitlements using resource profiles. A resource profile specifies the entitlements that cannot be requested or suggested by "suggested entitlements" lists.
- Chapter 12, "Requesting and Changing Access," on page 99 describes how to request and change access for yourself and other users, request creation of a new user in an Active Directory data source, request account password resets for yourself and other users, generate requests to terminate users and disable their accounts, generate requests to suspend access to accounts for users on leave of absence, generate requests to enable/disable and lock/unlock user accounts, and request fulfillment of business-source-specific commands that cannot be requested in RSA IMG but that can be fulfilled by AFX. This chapter is intended for all users who require the capability to manage access to your organization's entitlements.

Text Conventions

This guide uses the following text conventions:

Element	Convention Used	Example
Variables (The user supplies a value for the variable.)	*Courier and Italic* in angle brackets (<>)	Enter the following: `DISPLAY=<workstation name>:0.0 export display`
On-screen text	`Courier`	The following line displays: `path="/audit"`
User-typed text	`Courier`	Enter the following path name: `/etc/init.d/`
Cross-references	Underlined and hypertext-blue	See "Related Documents" on page 9.
References to documents (title and number)	*Italic*	*Installation Guide*

Related Documents

- *Installation and Upgrade Guide*
- *Database Setup and Management Guide*
- *Installation and Upgrade on WebSphere Guide*
- *Installation and Upgrade on WebLogic Guide*
- *Administrators Guide*
- *User Tasks Guide*
- *Collectors Guide*
- *Business Role Manager Guide*
- *Data Access Governance Guide*
- *Access Fulfillment Express Guide*
- *Access Fulfillment Express Connector Configuration Guide*
- *Public Database Schema Reference*
- *Novell Identity Manager Integration Guide*
- *Sun Identity Manager Integration Guide*
- *IBM Tivoli Identity Manager Integration Guide*
- *Onboarding Cloud Applications Guide*

Chapter 1: Introduction

Content

About Access Request Manager

Note: *See "Specifying System Settings" on page 36 in the Administrators Guide for information on how to enable the Access Request Manager module if you have purchased an Access Request Manager license.*

The Access Request Manager module enables line-of-business managers, supervisors, asset owners, and other users to request access and request changes to entitlements to resources in your organization for themselves and other users from multiple locations throughout the RSA IMG user interface. It also provides request management capabilities that enable you to customize how access is requested, create views of request activities (approvals and fulfillments) for business users who require monitoring capabilities over those activities, and specify policies that enforce policies for account password reset requests and manage challenge questions for login password reset requests.

Important: *The RSA IMG Rules module must be implemented on the system to provide decision support rules for access requests. All content related to business rules and violating access in this guide is applicable only if the Rules module is implemented on the system. Consult your RSA IMG administrator for more information.*

Feature Overview

Access Request Manager features:

- Enable requestors to request access and changes in access for themselves and for other users and to request account management action and user termination requests from multiple locations throughout the user interface.
- Schedule fulfillment of change request grants and revocations.
- Customize request workflows for applications, business units, data resource sets, directories, and role sets.
- Configure custom access request views of users and entitlements for different user types supervisors, business unit owners, application owners, role owners, and so on).
- Create account templates that define how an account is created for an application or a directory that requires that all entitlements to them must be granted through an account.
- Create custom request and submission forms.
- Create custom access request buttons.
- Create monitoring policies that specify views of approvals and fulfillment activities for particular sets of users.
- Create password policies that specify password strength standards for account password reset requests.
- Manage and implement challenge (or security) questions that users must answer to validate their identity when they request an RSA IMG login password reset if they forget their passwords.
- Specify the business source entitlements cannot request and to not appear in "suggested entitlement" lists.

Key Concepts

You should become familiar with the concepts described in this section before you, as an Access Request Manager administrator, configure Access Request Manager features or you, as an Access Request Manager user (access requestor), manage access for yourself and other users.

About Adding Access

Adding access for yourself or another user is the procedure where you initiate generation of a change request to grant entitlements (via accounts, application roles, role memberships) to yourself or another user. The actual fulfillment of the add access operation is dependent on the approval of users assigned to review and either endorse or reject the add request and the actual processing of the change in the external data source where user-entitlement associations are specified.

About Changing Access

Changing access for yourself or another user is the procedure where you initiate generation of a change request to either grant entitlements (via accounts, application roles, role memberships) to yourself or another user or remove them. The actual fulfillment of the add or remove access operation is dependent on the approval of users assigned to review and either endorse or reject the request and the actual processing of the change in the external data source where user-entitlement associations are specified.

About Suggested Entitlements

When you request access (for yourself or your subordinates for example), you are provided the option of selecting entitlements from a set of suggested entitlements that meets criteria for what a Access Request Manager administrator has deemed as potentially appropriate for the person for whom the request has been initiated. This criteria can be based on the entitlements or roles or both that other users who share one or more similarities with you have. These similarities can include affiliation with a department or business unit, a supervisor in common, or any other number of attributes shared by other persons in your organization.

For example, assume you have just joined the sales department in your organization. In a scenario where you would be required to request access to the entitlements you require to do your job, you would have the opportunity to request entitlements from a set of entitlements that are granted to members of the sales department. The fact that sales department members have these entitlements indicates that you should probably have them as well.

Important: *To comply with your organization's security policies, you may not want requestors to be able to view other users' entitlements in suggested entitlement operations. See* *"Specifying Access Request Settings" on page 18* *for more information on disallowing users from viewing other users' entitlements.*

About Scheduling Change Request Grants and Revocations

Access Request Manager enables you to specify a date on which you want an a request for an entitlement or a revocation of an entitlement to be processed in the data source containing user-entitlement associations. This enables you to request access in advance in the case of, for example, a user is moving to another department and you do not want him or her to have the entitlements the user requires in that department until he or she has actually joined the department. Conversely, you may want to request a change in access for the user that revokes the entitlement the user has in his or her current department on the date he or she actually leaves the department.

You can also specify that RSA IMG automatically generates a change request to revoke entitlements at a future date after they have been granted to a user. This enables you to ensure, for example, that a temporary employee or an employee in a transient job role only has the entitlements he or she requires for the required interval.

About Access Request and Decision Support Rules

RSA IMG provides decision support when you request or change access by comparing requests to the stipulations that specify who should have access to which entitlements in user access and segregation of duties rules that are deployed in the system. In other words, when you request access to an entitlement for yourself or any user RSA IMG checks the rules to determine whether the request would result in a violation of your organization's access security policies expressed by the rules.

If it does detect a potential violation, it generates an alert that appears on the Request Details window that includes:

- The rule that would be violated if the request were granted, an information link providing rule details, and any information provided with the rule.
- The user for whom violating access is requested.
- The violating entitlement's business source (application, role set, and so on).
- The violating entitlement and entitlement type.
- The conflicting entitlements for segregation of duties rules. An **Additional Information** link provides details about a conflicting entitlements.

Effective access request decision support depends on the deployment of rules that are designed to detect potential access violations. If decision rules are not implemented, access can be granted that may compromise your organization's security policies.

See Chapter 4, "Rules," on page 129 in the *User Tasks Guide* for information on creating and managing rules.

About Access Request Workflow Management

When an access request is submitted, RSA IMG generates a change request. A change request specifies the nature of the request, grant or remove access, and it is driven to completion by a multi-phase workflow that specifies who must approve and fulfill the request.

Access Request Manager enables business unit owners to create and edit custom submission and approval workflows for their business units, and it enables application, directory, role set, and data resource set owners to create and edit submission, approval, and fulfillment workflows for their objects. This empowers business managers with the ability to manage the workflow processes per their particular requirements.

See the following chapters in the *Administrators Guide* for more information:

- Chapter 11, "Creating and Managing Business Units," on page 157
- Chapter 12, "Creating and Managing Applications," on page 165
- Chapter 13, "Creating and Managing Directories," on page 181
- Chapter 19, "Managing Change Request Workflows," on page 247

See the following chapter in the *Data Access Governance Guide* for information on how to create and customize workflows for data resource sets:

- Chapter 3, "Managing Data Resources," on page 23

See the following chapter in the *Business Role Manager Guide* for information on how to create and customize workflows for role sets:

- "Customize Submission Form Information for a Role Set" on page 57

About User and Entitlement Views

Views define the user and entitlement choices available from selection windows you work with when you request access to entitlements or changes to entitlements. Access Request Manager administrators configure and manage views, and they can create as many views as necessary to meet the needs of users who require the ability to manage access for themselves and other users.

User Views

A user view specifies who can request access or change access for whom. A user view defines a set of users from which an access requestor can select users for entitlement add or change requests and the set of requestors who can access the view. Both sets of users can be based on user attribute criteria or criteria related to user-entitlement associations or both. You can create any number of user views to meet the needs of diverse user types in your organization who require the ability to request access and request changes to access.

For example, a user view could stipulate that only users who belong to a particular role and also have a particular set of entitlements can request and change access for users who belong to a particular group or business unit and who do not have one or more particular entitlements.

Entitlement Views

An entitlement view specifies who can request or change access to which entitlements for users specified in a user view. An entitlement view defines a set of entitlements from which an access requestor can select entitlements to add or remove for users selected from a user view and the set of users who can view and request access to entitlements in the entitlement set. The set of users who can view the entitlement set is based on user attribute criteria or criteria related to user-entitlement associations or both.

The set of entitlements from which requestors can request access can include all entitlements or any number of entitlements that meet various criteria, including but not limited to comparison of entitlement grants between similar users and specific entitlement attributes.

For example, an entitlement view could stipulate that only users who belong to a particular department can request access to entitlements that a particular group of users have who belong to a particular role.

About Customizing the Access Request Experience

Access Request Manager enables you to customize how access is requested and submitted in a variety of ways that you can implement to meet your organization's requirements for access to particular applications and for particular sets of users. For example: you can create custom request buttons that can invoke particular request forms or provide a series of request options; you can create custom request forms that guide a user through a series of steps required to request access; and you can customize the submission form to allow requestors to validate their requests by, for example, answering questions or providing a security code before they submit their requests.

About Providing Insight into Request Activities

Access Request Manager enables you to create monitoring policies that stipulate who can monitor the progress of request activities — request approvals and request fulfillments — delegated to users in your organization. For example, you may want to enable security officers in your organization to view, and in some cases take action on, activities delegated to a particular set of users or activities that involve a particular set of applications.

About Enforcing Account Password Reset Security Standards

Access Request Manager enables you to enforce password strength standards for business source account password reset requests by users. Enforcement is specified through a password policy. It stipulates the alphanumeric character standards for a password reset (length of password, number of numerals and uppercase characters in the password, and so on) and other restrictions such as the password duration resets using previously held passwords. You can create multiple and different password policies and associate them selectively to business sources, or you can associate a single policy to all business sources.

About Managing Login Password Reset Request Challenge Questions

When a user forgets his or her RSA IMG login password, the user can request a password reset from the login window. In response, the system requires the user to answer one or more challenge questions (mother's maiden name, first pet, and so on) to validate his or her identity and thus enable the user to login into the system with a new password. Users are required (and notified by system-generated email) to enroll their challenge question answers after they first log into the system. Access Request Manager enables you to specify which questions users must answer and the minimum number of questions users must answer from a set of challenge questions to successfully validate themselves when attempting a login password reset.

Chapter 2: Specifying Access Request Configuration Settings

Content

About Configuration Settings

In your role as an Access Request Manager administrator, you can specify the following change request settings:

- Global change request settings that allow you to:
  - Restrict self-service access request users from comparing their entitlements to other user's entitlements.
  - Disable access request operations from a user's details page.
  - Specify whether the system maintains versions of files attached to change requests and restricts attachments to particular file type extensions.
  - Associate custom or default request forms to application, business unit, data resource set, directory, entitlement view, and role set objects.

  See "Specifying Access Request Settings" on page 18 for more information.
- Manage the labeling of access request buttons, customize actions invoked by the buttons, and add and remove buttons. See Chapter 3, "Creating and Managing Access Request Buttons," on page 21 for more information.
- Create and manage the access request forms that users interact with when they request access. See Chapter 4, "Creating and Managing Access Request Forms," on page 27 for more information.
- Create and manage views of users and entitlements in change requests. See Chapter 5, "Creating and Managing Access Request Views," on page 41 for more information.
- Create and manage account templates. See Chapter 6, "Creating and Managing Account Templates," on page 49 for more information.
- Customizing global settings for request submission forms. See Chapter 7, "Customizing Request Submission Forms," on page 55 for more information.
- Create and manage monitoring policies for change request approvals and activities. See Chapter 8, "Creating and Managing Change Request Activity Monitoring Policies," on page 65 for more information.

Specifying Access Request Settings

Global access request settings specify access request capabilities available to users, how the system stores files attached to change requests, which file types can be attached to change requests, and the default request forms for different request source types.

To specify settings:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Settings**.

   Current settings appear.

3. Click **Edit**.

An editing session window appears. Configure the following settings as required:

- **Users Can Compare Access to Other Users** — Lets you specify whether the **Compare With User** option from the **Other Changes** button under the Access tab in a user details view is available to users requesting changes in access for themselves or other users. This is a global setting.

  You can, however, override this setting for any particular user view as described in Chapter 5, "Creating and Managing Access Request Views," on page 41. See "Requesting Changes in Access From the "Other Changes" Button" on page 104 for information on requesting changes in access based on comparison of user entitlements.

- **Allow Access Changes on a User's Detail Access Tab** — Lets you enable or disable availability of default "Remove," "Add Entitlements," and "Other Changes" buttons from a user's Access tab. This setting does not specify whether other request buttons can appear under the tab. See Chapter 3, "Creating and Managing Access Request Buttons," on page 21 for information on specifying the location of request buttons in the user interface.

- **Enable Change Requests on Group Attribute Changes** — Lets you enable the system to generate a request to change group attribute values in the data sources from which groups are collected. This applies to both managed and collected group attributes that have been designated as editable. See the *Administrators Guide* for more information:

  - Chapter 7, "Managing Attributes for RSA IMG Objects," on page 129 for information on how to designate collected group attributes as editable.

  - "Generate a Change Request to Update a Collected Group Attribute" on page 150 for information on how to initiate a change request to update group attributes.

- **User Attribute Used as the Person's Id in External Form Selectors** — Lets you specify the user attribute that identifies users in external form selectors.

- **URL Prefix to Use With External URIs** — Lets you specify the URL prefix to prepend to a URI string used for external form input validation.

- **Max Users Per Change Requests** — Lets you specify the maximum number of users for whom access can be requested in a change request. The default is unlimited users.

- **Support Versions for Request Attachments** — Lets you specify whether the system maintains file attachment versions.

- **Valid Extensions for Request Attachments (Comma Separated)** — Lets you restrict the file types (.doc, .png, and so on) that can be attached to a request. All file types can be attached if none are specified.

  See "About Attaching Files to Change Requests" on page 101 for more information.

  Note: *The file size limit for attachments is defined by the global "Max upload file size" setting under "Admin > System > Settings." The default limit is 10 MB. See the Administrators Guide for more information.*

- Specify whether to associate custom request forms or accept the association of default request forms with application, directory, entitlement view, role set, business unit, and data resource set objects in RSA IMG. The default is in effect for an object if no other form is associated with it. You can override form association on a per-object basis.

For example, if you associate form "A" as the default for applications the users who request access to an application interact with form "A" when they request access to an application. If, however, a form "B" has been associated with application "C," then requestors interact with form "B" when they request access to application "C." See Chapter 4, "Creating and Managing Access Request Forms," on page 27 for more information on designing custom forms for particular request scenarios.

Chapter 3: Creating and Managing Access Request Buttons

Content

About Managing Request Buttons

Users request access and changes to access using the request buttons located throughout the user interface. RSA IMG provides the following default access request buttons.

- **Add to My Access** — Lets users request access to entitlements for themselves.
- **Change My Access** — Lets users request changes to their entitlements.
- **Remove My Access** — Lets users request removal of their entitlements.
- **Reset My Password** — Lets users request a reset of the passwords for the accounts they have.
- **Add Access** — Lets users request access to entitlements for other users.
- **Change Access** — Lets users request changes in access to entitlements for other users.
- **Remove Access** — Lets users request removal of other users' entitlements.
- **Reset Password** — Lets users request a reset of the passwords for the accounts other users have.
- **Terminate User** — Lets users request an explicit termination of one or more users.
- **Terminate** — Lets users request an explicit termination of a particular user from the context of a user's details view.
- **Leave of Absence** — Lets users request an explicit leave of absence for a particular user.
- **Take a Leave of Absence** — Lets users request an explicit leave of absence for a particular user from the context of a user's details view.
- **Manage Accounts** — Lets users request that an account is enabled or disabled or locked or unlocked for one or more users.
- **Manage User's Accounts** — Lets users request that an account is enabled or disabled or locked or unlocked for a particular user from the context of a user's details view.

You can customize access request buttons to meet your requirements in the following ways:

- Create and remove buttons.
- Change button labels. For example, you may want to change "Change My Access" to "Change My Entitlements," or change "Add Access" to "Request Entitlements." This ability allows you to provide labels that conform with the lexicon in your organization pertaining to access and how it is granted to users within it.
- Group buttons as options under drop-down list buttons. You can create one or more drop-down list buttons that can each contain a variety of access request button options.
- Specify the locations where buttons appear, the home page dashboard or the Users menu or both locations and specify the order in which they appear.
- Specify the system action a button invokes. For example, you can specify that a button allows users to not only add and change access but to also invoke a URL or a change request form. See Chapter 4, "Creating and Managing Access Request Forms," on page 27 for information on forms.

- Specify which users can use the buttons, all or a sub-set of users. You may want to restrict a button to a set of users who, for example, are application owners or business unit owners.

Note: *Access request buttons were changed in product version 5.1 and 6.8. The aveksa-supplement-*.zip from the installation's packages directory now includes the following button definition files that you can use to reset v5.1 and v6.8 buttons and pre-v5.1 buttons on the user interface:*

- *RequestButtons/AveksaMetadata-5.0RequestButtons.xml to reset to the pre-5.1 style buttons.*
- *RequestButtons/AveksaMetadata-5.1RequestButtons.xml to reset to the 5.1 request buttons.*
- *RequestButtons/AveksaMetadata-6.8RequestButtons.xml to reset to the 6.8 request buttons.*

You can import the button files into your system using **Admin > Import/Export > Import**. See the *Administrators Guide* for more information.

Creating a Request Button

You can create as many request buttons as you require to meet your access request requirements.

To create a request button:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Request Buttons**.

   A list of request buttons appears.

3. Click **New**.

   The Create a New Request Button window appears.

4. Configure the button:

   - **Button Name** — Provide a name that indicates the action the button invokes. For example, if you want the button to invoke a particular change request form used for requesting access to Accounting department entitlements enter something like "Request Form-Accounting."
   - **Show** — Specify the placement for the button, as a **Button** on a page or as an option **Under a Drop-down** list on a page. For the latter option, provide a name for the drop-down, "Access Request-Accounting" for example.
   - **Location** — Specify the button (or drop-down list) location, **User Access** page or the **Requests** dashboard or both.
   - **Availability** — Specify who (which users) can use the button (or drop-down list). For example, if the button is intended for the Accounting department personnel specify users who belong to that department (Department = Accounting).

- **Action** — Specify the action the button invokes. Options include:
  - **Add Using Request Sources**: Specify the business sources from which entitlements can be requested by the button. For example, if you want this button to restrict requests for entitlements to the "Purchasing" application only, specify that application. Or if you want the button to restrict access to those entitlements from a particular entitlement view only, specify that entitlement view. You can also specify whether users can request access for themselves from the request sources by selecting **Self Service**.
  - **Change Using Request Sources**: Specify the business sources from which changes to entitlements that users have to those sources can be requested by the button. For example, if you want this button to restrict requests to change entitlements to the "Purchasing" application only, specify that application. Or if you want the button to restrict changes in access to those entitlements from a particular entitlement view only, specify that entitlement view. You can also specify whether users can request changes in access for themselves from the request sources by selecting **Self Service**.
  - **Select a Form from a List**: Specify a list of request forms invoked by the button from which the user can select a form.
  - **Go to a Form**: Specify a particular form invoked by the button.
  - **Go to a Reset Password Form**: Specify a particular reset password form invoked by the button. You can also specify whether users can request access for themselves from the request sources by selecting **Self Service**.
  - **Go to an External URL**: Specify a URL that is invoked by the button.
  - **Add to My Access**: Allows users to request access.
  - **Change My Access**: Allows users to request changes to their access.
  - **Remove My Access**: Allows users to request removal of their access.
  - **Add Access**: Allows users to request access for other users.
  - **Change Access**: Allows users to request changes to access for other users.
  - **Remove Access**: Allows users to request removal of access for other users.

5. Click **OK**.

Editing or Deleting a Request Button

You can modify all request button configuration settings. The changes take effect immediately after you complete the editing session. You can also delete buttons you no longer require.

To edit or delete a request button:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Request Buttons**.

   A list of change request buttons appears.

3. Select the button you want to edit or delete, and then:
   - Click **Edit** to modify the button. The Edit Request Button window appears. Proceed as follows:

     a. Modify settings as required.

     b. Click **OK**.
   - Click **Delete** to remove the button from the system, and then click **OK** in the confirmation window to complete the deletion.

Chapter 4: Creating and Managing Access Request Forms

Content

About Access Request Forms

When a user initiates a request (for access or changes in access, for a password change, and so on), he or she interacts with a request form. A request form can include any number of elements (text input fields, selection boxes, checkboxes, and so on) that a requestor can (or must) work with to generate the request. A request form may, for example, require the requestor to answer one or more questions or select one or more options before he or she can generate the request.

A form in its fully configured state consists of the following parts:

- Form Definition — Specifies a form's general properties: the form metadata, the form type, who the form is designed for (requests by the logged-in user or requests for other users or no users), custom workflow associations with form, the URI that can be used to validate information entered into a form by a requestor, and a namespace definition option for form variables (the fields in form) used in workflow processes. See "Creating a Form" on page 28 for more information.
- Form Fields — Specifies the elements on a form a requestor works with when completing a form. A field can be a text field in which a user must enter an answer to a question, a drop-down selection box or button from which a requestor must choose an, a table from which requestors can select options, static declarative text, and other diverse elements you can add to a form to guide the requestor through the access request process. See "Adding Fields to a Form" on page 31.
- Form Field Display Conditions — Specifies the criteria for displaying a field on a form and for enabling it on a form. You can build contingencies into your forms: specify that fields appear on a form based on the antecedent action a requestor took on another field. For example, you may want a field to appear that poses a particular question to a requestor if the requestor selects a particular option from a drop-down selection field. In some cases, you may also want a field disabled based on what input a requestor has provided or action taken on another field. For example, consider a field that requests a security code. You may want to disallow requestors from entering another code after the first entry. See "Conditionalizing and Enabling the Display of Fields on a Form" on page 35 for more information.

You can manage forms from the context of request sources. See the following for more information:

- "Manage Request Form Associations with an Application" on page 175 in the *Administrators Guide*
- "Manage Request Form Associations with a Business Unit" on page 161 in the *Administrators Guide*
- "Manage Request Form Associations with a Directory" on page 192 in the *Administrators Guide*
- "Manage Request Form Associations with a Data Resource Set" on page 31 in the *Data Governance Guide*

Creating a Form

You can create a diverse set of forms to meet your organization's various access request requirements.

To create a form:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Request Forms**.

   A table listing existing forms appears. RSA IMG provides a set of pre-defined default forms you can use or use as the basis for creating similar forms. You can edit default form fields, but you cannot edit default form general properties. You cannot delete default forms.

3. Click **Create Form**.

   The Create New Form window appears.

4. Specify how you want to create the form:

   - Create a form from scratch.
   - Create a form from another form by selecting the form you want to use as a template.

   Click **Next**.

5. Specify the form's general properties:

   - **Form Name** — Provide a name, preferably one that indicates the form's purpose.
   - **Description** — (Optional) Enter information about the form.
   - **Enabled** — Select to enable (default), or deselect to disable. A disabled form cannot be used for change requests. You would typically disable forms you plan to use in future particular use case scenarios.
   - **Form Type** — Specify the type of form you want to create if you are creating a form from scratch:
     - **Application**: Requests for entitlements and application roles for applications.
     - **Business Units**: Requests for entitlements for applications that belong to a business unit.
     - **Create Account**: Requests for new accounts. See Chapter 6, "Creating and Managing Account Templates," on page 49 for information on how to pre-define account properties for requests to create accounts.
     - **Data Resource Sets**: Requests for data resource access privileges for data resources that belong to a data resource set.
     - **Directory**: Requests for entitlements and application roles for a directory.
     - **Entitlement Views**: Requests for multiple levels of entitlements based on entitlement hierarchy relationships.
     - **Global**: Requests of any type. The Default Account Management Action form is of the global type.
     - **Provisioning**: Requests to provision new users into the system.
     - **Provisioning (Leave of Absence)**: Requests to change the access profile for users who are on a leave of absence.

- **Provisioning (Termination)**: Requests to remove the access profile for terminated users.
- **Register User**: Requests to create a new user in an LDAP (Active Directory) data source. See "Configuring the Register User Form" on page 87 for more information.
- **Reset Password**: Requests to reset an account password. See "Requesting an Account Password Reset for Yourself" on page 108 and "Requesting an Account Password Reset for Another User" on page 110 for more information.
- **Role Sets**: Requests for membership in roles in role sets.

For example, if this form is intended for access requests for applications only, choose Applications.

Note: *You cannot change the form type after you have associated a form with one or more business sources. For example, if a form's type is "directory" and you have associated it with a directory you cannot change the type to "business unit."*

- **Category** — (optional) Enter the name of a category in which to include this form. Organizing forms under categories enables you, for example, to invoke summary views of forms filtered by category, which is especially beneficial when you have numerous forms to manage.
- **Validation URI** — (Optional) Enter a Uniform Resource Identifier used to validate the form. Validation is processed by REST-style web service calls to URLs you provide in an external application. See "About External Form Validation" on page 36 for more information.
- **Workflow Variable Prefix** — By default, the name of the form is auto-filled for this setting and prepended to each of the field names in the form. You can accept the default or provide an alternative prefix. In either case, this prefix designates the fields in the form as private variables in workflows, which are formatted as follows:

  PublicData_workflow-variable-prefix_variable-name

  For example, a field named Field1 and a workflow variable prefix of Private would appear as PublicData_Private_Field1. If, however, you wanted to designate Field1 as public variable when you create that field for the form you would select the "Use avform prefix in workflow" option for the field. For example, this would be formatted as follows:

  PublicData_avform_Field1

- **Changes apply to** — Specify who this form applies to. Choose one of the following options:
  - **No users**: Select this option if this form is designed to complete tasks unrelated to requesting access for a user.
  - **Requestor**: Select this option if this form is designed for self-service requests by any user who can access this form.
  - **One user with the following attributes**: Select this option if you want this form to apply to change requests for a single user who has the attribute values you specify.
  - **Multiple users with the following attributes**: Select this option if you want this form to apply to change requests for users who have the attribute values you specify.

- **Request Grouping** — Lets you specify whether requests for access or changes to access for multiple users that are assigned to the same approver can be grouped into a single change request (default setting) or a change request is generated for each user.

  Select **All changes in one request** to enable change request grouping (default setting). Select **Changes by user** to enable a change request for each user.

- **Pending Request Visible** — Lets you specify whether the pending change request initiated through the form appears under a user's **Requests** tab. You typically might not want a pending termination request to be visible to a user for whom the request was generated.

- **Check outstanding requests** — Specify whether the requestor is prompted to include a change item in the request that is already included in a pending change request. If this option is disabled, the requestor is not prompted.

- **Approval Workflow** — Accept the default workflow, or select a custom approval workflow to associate with this form.

- **Fulfillment Workflow** — Accept the default workflow, or select a custom fulfillment workflow to associate with this form.

6. Click **Finish**.

   A details view of the form appears displaying the form's general properties under the **General** tab. At this point, you have created the form and saved it in the system. You can now add the fields (questions, text, prompts, input fields, drop-down lists, processing triggers, and so on) to the form that you want requestors to view and work with when they initiate a request. See "Adding Fields to a Form" on page 31 for more information.

Adding Fields to a Form

Fields are the elements on a form a user views and works with when they request access through a form. You can choose from a diverse collection of fields that enable you to build forms that enable you to customize the access request experience for particular sets of users requesting particular types of access.

To add fields:

1. Click **Fields** in a form's details view.

   If you are creating a form from scratch, no fields appear. If you are creating a form from another form, fields from the source form appear. You can modify or delete these fields and create new fields as required for the form.

2. Click the **New** button.

   The New Question window appears. The General tab is selected by default.

3. Provide a name for the question in the **Variable** field. You would typically provide a variable name that indicates the variable's purpose. For example, you might name a variable for a question that prompts a requestor to provide an attachment "Attachment Prompt."

4. Select the **Use avform prefix in workflow** option if you want to override the default prefix with the avform prefix to designate this field as a public variable in workflow processes; otherwise, deselect the option.
5. Select the element the user works with on the form to respond to the question from the **Control Type** field.

   For example:

   - You can select **Attachments** if you want to enable requestors to answer a question by uploading a file as the value of a field. This control includes the following configuration options:
     - Hide if empty: If selected, the Attachment field is not displayed on the request once the request has been submitted for approval.
     - Supports versions: If selected, the request stores multiple attachment versions.
     - Supports multiple files: If selected, the requestor can attach more than one file.
     - Valid extensions (comma separated): Specify that only files of a certain type (.docx, .png, and so on) can be attached. If no extensions are entered, any file type can be attached.
   - You can select **Attachments on Request** if you want to enable requestors to upload files to request at any point the request's lifecycle. This control includes the following configuration option
     - Hide if empty: If selected, the Attachment field is not displayed on the request once the request has been submitted for approval.

     Note: *See "Specifying Access Request Settings" on page 18 for information on configuring attachment on request settings.*
   - You can select the **Text** or **Large Text, Date,** or **Number** type to enable requestors to enter a response in a field to a question on the form.
   - You can select a **Drop-down**, **Radio Button**, or a **Picker** type to enable requestors to answer questions by choosing an option from a set of options. For a drop-down control type, you can specify whether drop-down options are listed alphabetically or in the order you specify.
   - You can select a **Static Text** type if you simply want to provide some information in HTML on the form, which could include hyperlinks and references to graphics. For example, you could use this type to state company guidelines for requesting access on a submission form and display your company logo.
   - You can select **Section Title** or **Horizontal Rule** if you want to create graphical user interface elements for the form.
   - You can select **Reset Shared Password** if you want to provide a checkbox in the form its user can select to generate a change request to reset a password for shared accounts in an account management form.
   - You can select **Set Variable (Non-Visual)** control if you want the control to set a specific variable to a specific value. Form users can update the value of that variable, but if the user

goes to the next page and then browses back to the previous page the control is again set to the originally specified value.

Note: *Use a hidden text field to retain a modified variable value.*

- You can select **Password Field** if you want to create a text field in which a password is entered manually by the requestor or is generated by a password generator specified in the **Password Generator URI** field. The password generator appears as a button on the form. When it is clicked, the URI enters the password to the password field.

  You can specify a password validation source in the **Validation URI** field. You would typically use this field in a request designed to create an account to a resource in your organization or to add a new user to an user identity source in your organization. For the former case, you would typically also create a text field for a username. In the latter case, you would typically also create text fields for user attributes required in a user identity record.

  Once a request that includes the password field is generated, the system encrypts the password. It does not appear on any of the change request approvals in the workflow. It does appear to the request fulfiller who requires knowledge of the password to complete the request and in the email the system generates for the users who require the password (the requestor or the person for whom the request was generated).

Configuration options vary for different control types. For example, where a Text control type includes but a few configuration options an **Entitlement Table** and an **Account Table** control type includes multiple configuration options that allow you to control how users can interact with a form that includes these selection tables. For example:

Common to both control types:

- **Hide table if empty** — Lets you specify that an empty table is not displayed in the form.
- **Allow table grouping** — Lets you specify a default grouping option for the table. This option if set to other than "None," cannot be deleted on the table by users who pick items from the table. Users can, however, specify additional grouping options.
- **Display search tools on table** — Lets you specify whether the table includes the Search field.
- **Display column selection and table options** — Lets you specify whether the table includes the Table Options feature.

Entitlement Table type:

- **Show child entitlements of** — Lets you specify the entitlement table containing the parent entitlements. This pertains only to entitlements that have been organized in a parent-child hierarchy. See "Managing Entitlement Request Hierarchy Relationships" on page 198 in the *Administrators Guide* for more information. In this case, only those entitlements that are child entitlements of the parent table you specify would appear in the table.
- **Entitlement Rule** — Lets you filter the entitlements to display in the form.
- **Change Item Handling** — Lets you specify restrictions on the number of entitlements that can be selected. For example, the **Subject Must Have One Entitlement** option specifies that only one entitlement can be selected.

- **Create change items even when hidden** — Lets you specify that entitlements selected in an entitlement table that is subsequently hidden per a condition on the table are included in the change request that is submitted.

Account Table type:

- **Show account management lock action** — Lets you specify that users can perform an account locking action in the form.
- **Show account management unlock action** — Lets you specify that users can perform an account unlocking action in the form.
- **Show account management enable action** — Lets you specify that users can perform an account enablement action in the form.
- **Show account management disable action** — Lets you specify that users can perform an account disablement action in the form.
- **Account Filter** — Lets you filter the accounts to display in the form.

  Note: *See "Requesting Account Management Actions" on page 112 for information on working with account management actions in a form.*

A **User Account Table** control type includes several of the configuration options included in Entitlement Table type. Given its inclusion in the Default Reset Password form that users interact with when they request resets of the passwords to business source accounts, the **Allow multiple selections** option if enabled allows requestors to request a password reset using a single password for multiple accounts. (Not recommended for security reasons.)

A **Provisioning Command (Non-Visual)** control type lets you specify a business source nd the commands supported by that business you want fulfilled on the business source via an AFX connector.

Note: *See "Requesting Fulfillment of Business-Source-Specific Commands" on page 113 for information on requesting fulfillment of business-source-specific commands.*

A **Naming Policy Transform (Non-Visual)** control type lets you specify a naming policy to implement for a register user form type.

A **Register User Command (Non-Visual)** control type lets you specify the input parameters to create a new user for the register user form type.

Note: *See Chapter 10, "Set Up the System for New User Registration Requests," on page 81 for information on working with the Naming Policy Transform (Non-Visual) and the Register User Command (Non-Visual) fields.*

6. Enter the text you want to appear on the form in the **Question** field. For example, if you create a drop-down button that enables requestors to choose from multiple options you would typically enter a question that prompts the requestor to choose an option. You can, of course, enter imperative statements in the field as well.
7. (Optional) Enter tooltip text in the **Tooltip** field. The requestor can display the tooltip on the form by placing the cursor over the question.
8. (Optional) Select **Required** if requestors must respond to the question on the form to proceed with the access request process. This option is not available for non-visual controls.

9. (Optional) Specify one or more conditions for the question. A condition defines the circumstances under which a question appears on a form. See "Conditionalizing and Enabling the Display of Fields on a Form" on page 35 for more information.
10. Click **OK** to add the field to the form.

    The field appears in the Field tab table.
11. Use the arrows (up, down, top, bottom) in the table to specify where in a sequence of fields you want this field located.

Conditionalizing and Enabling the Display of Fields on a Form

You can specify one or more conditions that stipulate whether a visual control field appears on a form. In the case of multiple conditions for a field, only one condition must be met. You can also specify whether the field is enabled or disabled on the form at any stage during requestor interaction with the form based on conditions.

For example, you may want a field to appear to requestors who have provided a particular answer to a question posed by another field on a form. Furthermore, you may also want the system to disable a question field or selection drop-down field after a requestor has interacted with the field or enable a field only if some prior condition has been met.

To create a condition:

1. In a form's details view, click **Fields.**
2. Click **Edit** for the field for which you want create a condition.
3. Click **Display** in the field's details view.
4. Click **New Condition**.

   A set of condition configuration options appears.
5. Specify the criteria that must be met for this field to appear on the form:
   - Does <another field|a requestor attribute|a request source attribute|. . .> have a value? If yes, display this field.
   - Does <another field|a requestor attribute|a request source attribute|. . .> not have a value? If yes, display this field.
   - Does <another field|a requestor attribute|a request source attribute|. . .> equal| does not equal|is greater than|is less than|is greater than or equal to|is less than or equal to> a particular value? If yes, display this field.
   - Does JavaScript Expression include the <value from the attribute selection drop-down>. If yes, display this field.

   The answers to multiple questions must all be true for this condition to be applied.
6. Click **OK** to apply this condition to the form.

To specify when a field is enabled or disabled:

1. In a form's details view, click **Fields.**
2. Click **Edit** for the field for which you want create a condition.

3. Click **Enabled** in the field's details view.
4. Click **New Condition**.

   A set of condition configuration options appears.
5. Specify the criteria that must be met for this field to be enabled on the form as you did for specifying field display criteria.
6. Click **OK** to apply this condition to the form.

About External Form Validation

External form validation comprises both field and form validation.

Field Validation

For field validation, the URI is called with three parameters:

- name — The Variable Name defined on the field.
- question — The Question defined on the field.
- value — The value for the name/question to test.

If there is an error, the error should reference the question. For no error, the response should be empty (whitespace is ignored). If the URI does not include the schema, hostname, and port, these are added.

For example, if you have a demo.war with validatephone.jsp script that validates a phone number provided by a form user in response to question on the form and this application is accessible on the same server as "/demo," then the Validation URI should be /demo/validatephone.jsp, and validatephone.jsp would look similar to the following:

```
<%

    String name = request.getParameter("name");

    String question = request.getParameter("question");

    String value = request.getParameter("value");

    if (!value.matches("[(][0-9][0-9][0-9][)]
?[0-9][0-9][0-9]-[0-9][0-9][0-9][0-9]")) {

        out.println("Invalid phone number for " + question + ", expected (###)
###-####");

    }

%>
```

Form Validation

For form validation, the URI is called with two parameters for each field:

- value.variable — The name contains the value.
- question.variable — The name contains the question.

Form level validation also includes the attributes of key objects:

- avform.application.<attributes> — The associated application object (if application form)
- avform.businessunit.<attributes> — The associated business unit object (if business unit form)
- avform.requestor.<attributes> — The logged in user making request
- avform.users[index].<attributes> — The target users (only index 0 if there is one user)

Because of the large number of parameters, this request uses the POST method. Attributes that have null values do not have their parameters added. If there is an error, the error should take the form:

- error.variable-name1=error message
- error.variable-name2=error message
- error=A global error message, if one is needed

For example, if you have a demo.war with validateform.jsp and this application is accessible on the same server as "/demo," then the Validation URI should be /demo/validateform.jsp and validateform.jsp would look something like:

```
<%@ page import="java.util.Enumeration" %>

<%@ page import="java.util.HashMap" %>

<%

    HashMap<String, String> values = new HashMap<String, String>();

    HashMap<String, String> questions = new HashMap<String, String>();

  // Make the parameters and questions easy to access

  for (Enumeration e = request.getParameterNames(); e.hasMoreElements();) {

        String name = e.nextElement().toString();

        String value = request.getParameter(name);

        if (name.startsWith("value.")) values.put(name.substring(6), value);

        if (name.startsWith("question.")) questions.put(name.substring(9), value);

    }

    if (!values.containsKey("something else")) {

        out.println("error=Where is the something else field!");

        return;

    }

    if (!values.get("something else").contains("Important")) {

        out.println("error.something else=Where is the \"Important\" in " +
questions.get("something else"));

        return;

    }
```

%>

External Validation Warnings

- If any form validation request takes more than 3 seconds, a warning is displayed in the log output.
- If the total external validation request takes more than 3 seconds. a warning is displayed in the log output.
- If the total external validation time takes more than 3 seconds, a warning is displayed in the log output.

All external validation is logged with the category com.aveksa.gui.ExternalValidation.

Setting Up Your Own WAR

If you are using JBoss, you can just create a directory at /home/oracle/jboss/server/default/deploy such as demo.war. When you do this, any file that you put in that directory will be available through the application server with an URL like http://hostname/demo/file-in-demo.war. The name "demo" was derived from "demo.war". This can contain form selectors, field validations, form validations, and list control data sources.

Managing Form Associations with Request Sources

Note: *You can also manage form associations for particular request sources from the context of those sources.*

When you associate a form with a request source, you specify that requests for access to the request source invoke the form associated with the source.

If you associate multiple forms to a request source, a requestor can choose a form from a selection dialog box that appears when the requestor clicks on the request source from a request source table. You can assign forms to multiple request sources, and you can unassociate forms from request sources.

To manage form associations with request sources:

1. In a form's details view, click **Associations.**

   The Associations window appears. It lists request sources.

2. Select the request sources you want to associate with the form or unassociate from the form.

   The Selected request sources box lists the request sources you selected.

3. Associate the form to or unassociate the form from the request sources:
   - To associate, click **OK**.
   - To unassociate, click **Remove All**.
4. Click **OK**.

Editing or Deleting a Form

You can edit and delete all user-created forms. You cannot delete RSA-provided default forms. You cannot edit default form general properties, but you can edit form field configurations.

To edit or delete a form:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Request Forms**.

   A table listing existing forms appears.

3. Click the name of the form you want to edit or delete, and then:

   - Click **Edit** to modify the form. The Edit Request Form window appears. Proceed as follows:

     a. Modify settings as required. See "Creating a Form" on page 28 for information on form general property settings.

     b. Click **Finish**.

   - Click the **Delete** icon (trashcan) to remove the form from the system, and then click **OK** in the confirmation window to complete the deletion.

See "Adding Fields to a Form" on page 31 and "Conditionalizing and Enabling the Display of Fields on a Form" on page 35 for more information form field configuration.

Chapter 5: Creating and Managing Access Request Views

Content

About Access Request Views

When users initiate an access request or a change in access for another user, they are provided with a view of the users for which they are authorized to request or change access. When they request or change access for themselves or other uses they are also provided a view of entitlements they are authorized to request or remove. The views available to requestors are specified by the following access request views:

- User Views
- Entitlement Views

User Views

A user view specifies the list of users displayed in a request form and who can access the list when they initiate an access request or change access action. In other words, a user view specifies the particular set of users who can manage access for a particular set of other users. The possible criteria on which a user view can be based are extensive. Any number of user attributes or affiliations with entities in your organization can dictate who can manage access for whom. You can create any number of user views and also modify user views to meet your particular access management requirements.

For example:

- A user view could specify that only members of a particular department, business unit, role, or group who are supervisors can manage access for subordinates and who share the same memberships.
- A user view could specify that users whose Job Code attribute value is "Contractor Employee Access Director" can manage access for users with a Job Status attribute value of "Consultant" or "Temporary."
- A user view could specify that users whose Location attribute value is "New York" and whose Job Code attribute value is "Role Security Manager" can manage access for all users who are members of the "Northeast Sales" and "Northeast Customer Service" roles.
- A user view could specify that supervisors can manage access for only those users who have rule violation counts that exceed a particular threshold.
- Additionally, you can specify whether to disallow a user view from being used in a user comparison operation in a change access procedure when the global setting for user comparison is enabled. And you can also specify that a view can be used in generic user selection windows.

The previous examples illustrate the flexibility you have in designing user views that meet the diverse access request management requirements of the members of your organization.

See "Creating a User View" on page 44 for information on creating user views, see "Editing View Configuration Settings" on page 47 for information on modifying views, and see "Delete a View" on page 48 for information on deleting views.

Out-of-the-Box User Views

Access Request Manager provides the following pre-configured user views for users who request access for other users:

- **Direct Subordinates** — This view lists users who are direct subordinates of the user who wants to request access or change access.
- **Active Users** — This view lists all users in the system who are currently employed by your organization to whoever wants to request access or change access.
- **All Users** — This view lists all users in the system, regardless of whether they are employed or not employed by your organization, to whoever requests access or changes access.

These views are provided as options in all add access and change access request forms. In other words, the access requestor can select the user view he or she wants to use. They can be customized to meet your requirements, and they can also be leveraged as a learning aid for creating user views by exemplifying how a user view can be configured.

Entitlement Views

An entitlement view specifies the list of entitlements displayed in a request form and who can access the list when they initiate the request. In other words, an entitlement view specifies the particular set of users who can manage access to a particular set of entitlements that can be granted to themselves or other users.

The possible criteria on which a entitlement view can be based are extensive. Any number of users can be authorized to view entitlements based on their type. You can create any number of entitlement views, modify entitlement views, and specify a limit on the number of entitlements that can be displayed in a selection list of entitlements to meet your particular access management requirements.

Out-of-the-Box Entitlement Views

Access Request Manager provides the following pre-configured entitlement views:

- **Suggested Entitlements** — This view lists entitlement that similar users have.
- **All Entitlements** — This view lists all entitlements in the system.

Accessing User and Entitlement Views

You can access summary and details views of access request user and entitlement views at any time.

To access a summary view of user and entitlement views:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Entitlement Views** to display all entitlement views created in the system and the order in which they appear in the entitlement view selection box in an access request form. Click **User Views** to view all user views created in the system and the order in which they appear in a user view selection box in an access request or change access form.

3. Click the name of a view to view configuration details.

Creating a User View

You can create as many user views as required to meet your organization's requirements for enabling users to request and change access.

To create a user view:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **User Views**.

   A list of user views appears. The views are listed in the order they appear in the drop-down list in an add access or change access form for the users for which they are intended. By default, when you create a new user view it is appended to the end of the list. See "Specifying the Order in Which Views Appear in a Form" on page 47 for information on how to rearrange the order.

3. Click **Create View**.

   The Create View window appears.

4. Configure the following settings:

   - **Name** — The identifier for the view. For system use only.
   - **Display Name** — The view name displayed in a request form.
   - **Users who will see this view** — The users authorized to view the list of users available from the view in a request form. You specify the users based on user attribute value similarities and shared membership in groups and roles.
   - **Initial set of users to show** — The set of users that can appear in a request form. User sets include:
     - **All** — All users whether terminated or not.
     - **Active** — Users whose identities are in the system and who have not been terminated.
     - **Inactive** — Users whose identities are in the system and who have been terminated.
     - **Subordinates** — Users who report directly to the supervisor who is the current login.
   - **Users of initial set to show** — The set of users from the initial set of users based on the filtering criteria you specify. For example, if you chose "All" for the initial set of users to show you can filter the set further by specifying that only members of a particular department are displayed.
   - **Preview User** — The user you want to specify for the **Preview** action. The preview of the user view that appears is what the user you specify sees when he or she accesses the view during a request action.
   - **Used for generic user selection screens** — Use this option to specify whether this user view is available in any request window.
   - **Used for comparing users** — Use this option to disallow this view (deselect) from being used in comparing users operation in change access procedures. This option allows you to override the global option set to allow all user views to be used in comparison operations.

You cannot enable comparison for a user view if the global comparison option is disabled. See "Specifying Access Request Settings" on page 18 for more information on the global comparison option.

5. Preview the view you configured, make changes as necessary, and then click **OK**. See "Previewing a View" on page 46 for more information.

Creating an Entitlement View

You can create as many entitlement views as required to meet your organization's requirements for enabling users to request and change access.

To create an entitlement view:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Entitlement Views**.

   A list of entitlement views appears. The views are listed in the order they appear in the drop-down list in an add access or change access form for the users for which they are intended. By default, when you create a new entitlement view it is appended to the end of the list. See "Specifying the Order in Which Views Appear in a Form" on page 47 for information on how to rearrange the order.

3. Click **Create View**.

   The Create View window appears.

4. Configure the following settings:

   - **Name** — The identifier for the view. For system use only.
   - **Display Name** — The view name displayed in a request form.
   - **Users who will see this view** — The users authorized to view the list of users available from the view in a request form. You specify the users based on user attributes and shared membership in groups and roles.
   - **Initial set of entitlements to show** — The set of entitlements that can appear in a request form. Entitlement sets include:
     - **All** — All entitlements available in the system.
     - **Similar Users** — All entitlements similar users have.
     - **Matching** — All roles for which the user has matching entitlements.
     - **Similar Users and Matching** — All entitlements of similar users and roles for which the user has matching entitlements.

     Similarity of users is based on the shared values for the user attributes you specify. For example:

     - Similar Users Attribute 1 (Users with a Department attribute value of "Accounting")
     - Similar Users Attribute 2 (Users who have a Job Code attribute value of "Manager")

- Similar Users Attribute 3 (Users who have a Location attribute values of "New York")

In this case the entitlements that users in New York who are also managers in the accounting department have are available for selection in the request form.

- **Entitlements of initial set to show** — The set of entitlements from the initial set of entitlements based on the filtering criteria you specify. For example, if you chose "All" for the initial set of entitlements to show you can filter the set further by specifying that only entitlements for a particular application are displayed.

  By default, all entitlement types (**Include Application Entitlements**, **Include Application Roles**, and so on) listed are selected and are available in a request form. You can filter which entitlements are available by deselecting those you do not want.

  You can also specify that the **Allow view to be used with Add entitlements for an application** option is available in a request form.

- **Preview User** — The user you want to specify for the **Preview** action. The preview of the entitlement view that appears is what the user you specify sees when he or she accesses the view during a request action.

- **Preview Application** — The preview view filtered by a particular business source. This filter does not influence the actual view of entitlements requestors can view and select in a request. It simply allows you, the preview user, to view entitlements in smaller chunks on a per-application/directory basis when you preview entitlement views.

5. Preview the view you configured, make changes as necessary, and then click **OK**. See "Previewing a View" on page 46 for more information.

Specify the Maximum Number of Entitlements and Groups Displayed in an Entitlement View

For any entitlement view that access requestors can invoke, you can specify the limit on how many entitlements and groups can appear in the view. The default is 100,000 entitlements and 1000 groups.

To specify the maximum allowed:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Entitlement Views**.

3. Click **Edit**.

   A Settings window appears.

4. Enter a maximum number or rows and groups, and then click **OK**.

   The setting applies to all entitlement selection lists invoked in change requests.

Previewing a View

The preview feature enables you to configure default settings for the selection table that appears in the access request or change access form based on the view and examine what a user specified by the Preview User setting sees in a form.

To preview a view:

1. Click the **Preview** button.
2. Configure table settings as necessary. See "Working with Table Options" on page 28 in the *Administrators Guide* for more information.
3. Note any corrections required to the view configuration based on what appears in the preview.
4. After you have made any corrections to the view configuration, you can preview again to verify that the form is valid.

Specifying the Order in Which Views Appear in a Form

Users are provided one or more user and entitlement view selection options when they initiate a request. You can specify the order in which these view options appear in user view and entitlement selection boxes. This is especially important if there are many view options available and you want requestors to find the views most relevant to them without too much difficulty.

To specify the order of views:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.
2. Click the tab for the view type you want to order.
3. Use the paging arrows (up, down, top, bottom) to rearrange the order.

   The order is reproduced in the view selection boxes in a request form.

Editing View Configuration Settings

You can edit all user and entitlement view configuration settings.

To edit view configuration settings:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.
2. Click the view type tab to display the view you want to edit.
3. Click the name of the view you want to edit.
4. Click **Edit**.

   The Edit View window appears.
5. Edit settings as required, and then click **OK**.

   The edits go into effect immediately.

Delete a View

In some cases you may want to delete views you no longer require.

To delete a view:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.
2. Click the view type tab to display the view you want to delete.
3. Click the name of the view you want to delete.
4. Click the **Delete** icon (trashcan).

   The view is removed from the system.

Chapter 6: Creating and Managing Account Templates

Content

About Account Templates

Note: *The "business source" term in this chapter refers to either an application or a directory.*

An account template lets you specify the account properties you want included in an account that is created for a business source during the manual fulfillment phase of a change request. This lets the business source technical owner hide most of the account implementation details from the requestor, while allowing certain business-related information to be provided by the requestor. A business source can be accessed by multiple account types. For example, an administrator account providing access to an application typically includes greater privileges to the business source than does a basic user account. Therefore, an account template designer must know which account parameters to include in different template types to fulfill account creation.

Account Template Association with a Business Source

To accommodate the different account types that can be created for a business source, one or more account templates that define properties for the different account types can be associated with a business source. When a requestor requests access to it, he or she can choose the appropriate account template during the request process for the type of account he or she wants to create.

Account template options for requestors are available only if the business source's **Entitlements Require Account** setting is enabled. This setting enforces the rule that any entitlement request for the business source be granted to an account and not directly to a user. If necessary, a create-account item is added to the request. See "Managing How Requests Are Processed for an Application" on page 175 or "Managing How Requests Are Processed for a Directory" on page 191 in the *Administrators Guide* for more information.

Account Templates and Access Fulfillment Express

If you are implementing Access Fulfillment Express (AFX) to automate create account change request fulfillment activities for business sources, an account template provides the inputs required to manually complete them if auto-fulfillment fails. In this case the fulfiller who creates an account has the information required. You would typically design account templates to include the same parameter-value pairs that the auto-fulfillment connector includes. See the *Access Fulfillment Express Guide* for more information on implementing AFX capabilities with business sources.

Account Templates and Form-Driven Modifications During the Request Process

You can associate a "create account" form to an account template. The form can be configured to enable requestors to provide or modify one or more default parameters specified by the account template with which it is associated during the request process. For example, you could create a form that allows a requestor to overwrite or provide a default password value. A form of this sort might also display read-only values that a requestor should not be allowed to change but might be required to confirm as valid via questions configured in the form.

Another aspect of the form-template association allows you to specify that changes a requestor makes to default account template values in a form are propagated to the template. This, essentially, provides "on-the-fly" editing capability to requestors on an account template.

Account Templates and Rule-Generated Change Requests

No user interaction is required or possible for a change request that is generated by the RSA IMG rules engine. (A change request to add members to a role is triggered by a role membership rule for example.) In the case where the rules engine generates a change request to add entitlements to an application or a directory and either resource requires that entitlements to it must be granted via accounts only, you can create a "rule account template" that specifies the necessary create account information in the change request and associate it with the resource.

With one important exception, the rule account template can be configured like any other account template. Because no user interaction is possible for the rule-generated change request, the rule account template must not be associated with a form (which requires user interaction). See "Managing How Requests Are Processed for an Application" on page 175 or "Managing How Requests Are Processed for a Directory" on page 191 in the *Administrators Guide* for information on associating a rule account template with an application or a directory.

Creating an Account Template

You can create as many account templates as your organization requires to fulfill creation of different account types. Account template creation summary:

1. You create the basic framework of an account template as described below.
2. Then you must specify the inputs (the account parameters or properties) used to create the account in the target data source as described in "Add Parameters to the Account Template" on page 52.

At any point in the process, you can opt to set up an association between an account creation form and the account template that allows a requestor to modify parameter values in a create account request and also automatically update those values in the account template. See "Manage Form Association with an Account Template" on page 53 for more information.

To create an account template:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.
2. Click **Account Templates**.
3. Click **Create Account Template**.

   The Account Template window appears.
4. Configure the following properties:
   - **Name** — Enter a unique name.
   - **Description** — (Optional) Enter a description of the purpose of the template.
   - **Is Service Account** — Specify whether this is a template for a service account. A service account does not require that any users have the account and that it should not be removed if no user has the account. For example, a service account might be one that logs a web server into a database.

- **Account Creation Form** — (Optional) Select the account creation form you want a requestor to interact with when he or she initiates a requests that involves creation of an account. (A business source may require that entitlements to it can only be granted via an account. Therefore, a request for an entitlement to the business source would also generate a request to create an account for the entitlement.) This form would typically be configured to include fields that correspond to some or all of the parameters you specify in an account template.

  Important: *Do not associate a form with an account template designed to be a "rule account template."*

  Furthermore, the form fields can be editable and the edited parameter values can be propagated to the account template. If no form is specified, the request is generated with the default values from the account template. See "Manage Form Association with an Account Template" on page 53 for more information.

5. Click **OK**.

   The account template entry appears in the Account Template window table. To complete configuration of the template, you must add account parameter-value pairs to the template that define the account. See "Add Parameters to the Account Template" on page 52 for more information.

Add Parameters to the Account Template

You can add all account parameter-value pairs required to create accounts in a business source (Active Directory or LDAP for example).

To add parameters to a template:

From the Account Templates window, click the name of the template.

A details view of the template appears. It lets you specify both input and pending account parameters:

- To add an input parameter:

  1. Click **Add Parameter**.
  2. Enter a name and a value for the parameter.
  3. (Optional) Select the field that corresponds to this parameter in the **Form Field** drop-down if you want to link a form field to the parameter. This is applicable only if you have a form associated with the account template. If selected, the value entered on the form is used when creating the account. See "Manage Form Association with an Account Template" on page 53 for more information.
  4. Click **OK**. Repeat for each parameter you want to add to the template.

- To add a pending account parameter, click **Add Pending Account Parameter** and enter a name and a value for the parameter. Click **OK**. Repeat for each pending account parameter you want to add to the template. Pending Parameters are used to fill in the RSA IMG data for the account, so that the account can be used by RSA IMG before it is collected. This lets the user request entitlements for the account before it is collected.

Manage Form Association with an Account Template

You would associate an account creation form with an account template if you want to provide a requestor the ability to change parameter values specified by the account template during the request process, or perhaps to allow the requestor to simply confirm the validity of the parameters. For any account template parameters that do not have a corresponding form field, the default value on the template is used.

Once you have defined the account template and configured its parameter specifications, you can manage a form associated with an account template in the following ways:

- Create a "create account" form that includes fields that correspond to parameters in the account template. For example:
  - The account template includes Name, ID, and Password parameters.
  - The account creation form includes corresponding Name, ID, and Password fields. To ensure that default values from the account template appear in the form when it loads during the request process, select the "AccountTemplate" type variables as default values for the fields in the form. For example, you would select ${avform.AccountTemplate.Name} for the Name field, ${avform.AccountTemplate.ID} for the ID, and so on.
  - The fields can be editable or read-only.
  - The form is selected from the account template's Create Form drop-down.
  - The form is available to requestors when a create account request is generated.
- Enable updates to a form associated with an account template to update parameter values in the account template. For example:
  - The account template includes Name, ID, and Password parameters.
  - The account creation form includes corresponding Name, ID, and Password fields.
  - The **Form Field** setting for the parameters must specify their corresponding form fields.
  - Changes made by a requestor to parameter values in the form associated with the account template are used when generating the change request.

Editing or Deleting an Account Template

You can edit account templates as necessary, and you can delete those you no longer require.

Note: *You can also edit an account template from the context of a business source that has the account template associated with it. See* *"Managing How Requests Are Processed for an Application" on page 175* *or* *"Managing How Requests Are Processed for a Directory" on page 191* *in the Administrators Guide for more information.*

To edit or delete an account template

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Account Templates**.

   A list of account templates appears.

3. Open the details view of the account template you want to edit or delete, and then do the following:
   - Click **Edit** to modify the account template. The Edit Account Template window appears. Proceed as follows:
     a. Modify settings as required. See "Creating an Account Template" on page 51 for information on account template settings.
     b. Click **OK**.
   - Click the **Delete** icon (trashcan) to remove the account template from the system, and then click **OK** in the confirmation window to complete the deletion.

Chapter 7: Customizing Request Submission Forms

Content

About Request Submission Forms

You can customize the request submission form that requestors complete when they request access and changes to access for themselves or other users. You can specify the following global settings for the request submission form:

- Provide a notes field in which requestors can enter comments.
- Display attribute values for requests.
- Allow requestors to specify a request revocation date (for temporary access) and a fulfillment date (for delayed access) on a request form.
- Specify who can view business rule violations that would occur if a request were fulfilled, who can submit those requests, and whether violations are generated on the source for indirect entitlements in a role.
- Specify whether requests for access or changes to access for multiple users that are assigned to the same approver can be grouped into a single change request (default setting) or are grouped into a change request for each user.

You can also configure additional information elements (fields and controls) for submission forms that enable requestors to provide information helpful to or required by request approvers and fulfillers to process a request. These elements can be conditionalized so that they appear only on the submission forms for particular requestors or for requests for access to particular assets. For example, you may want to include the following information elements on submission forms that enable or require the requestor to do the following:

- Answer questions about the request.
- Attach files to the request.
- Enter a validation or security code.
- Accept a terms of use agreement.

Also, information elements can be customized for the following objects on a per-object basis:

- Applications
- Business units
- Data resource sets
- Directories
- Role sets

For example, an application owner may want to solicit other types of information for his or her resource, information that would not be forthcoming from the global request submission form. Conversely, the owner may want to remove irrelevant globally configured information fields from the form.

Configuring Global Request Submission Form Settings

You can configure which options appear on all request submission forms.

To configure settings:

1. Click the **Requests** menu and select **Configuration**.
2. Click **Submission**.

   The Submission settings page appears. It displays current settings.
3. Click **Edit Settings**.
4. Configure the following settings:

   - **Instructions** — Modify the instructions that appear on a change request's Request Details window as required.
   - **Description can be specified for the request** — Lets you specify whether access request submission forms include a Description field where text can be entered.
   - **Notes can be specified for the request** — Lets you specify whether access request submission forms include a Notes field where commentary can be entered.
   - **Notes are required for the request** — Lets you specify whether access request submission forms that include a Notes field requires the requestor to enter commentary. This option can be selected only if the "Notes can be specified for the request" option is selected.
   - **Request attributes are shown in the submission form** — Lets you specify whether access request submission forms include attributes that requestors can set values for. See Chapter 7, "Managing Attributes for RSA IMG Objects," on page 129 in the *Administrators Guide* for more information on creating attributes for change requests.
   - **Users can specify a date changes should not be fulfilled before** — Lets you specify whether access request submission forms include a configurable request fulfillment date proviso. The fulfillment date enables access requestors to specify the date on which fulfillment of an access request should be completed. Requestors may want to delay fulfillment of a request for a variety of reasons (because a user who is scheduled to move from one department to another does not require access to his or her new department's resources until he or she actually joins the new department for example).
   - **User can specify a date when added access should be revoked in a secondary request** — Lets you specify whether access request submission forms include a configurable entitlement revocation date proviso. The revocation date enables access requestors to specify a date on which a change request should be automatically generated to revoke an entitlement grant fulfilled by the request. This enables access requestors to essentially request temporary access (for temporary employees for example).
   - **Show violations to the specified requestors** — Lets you specify the requestors who would be informed that a request would result in a rule violation if the request were approved and fulfilled. This setting is applicable only if user access or segregation of duties rules are implemented on the system.

- **Requests with violations can be submitted by requestors** — Lets you specify the requestors who would be allowed to submit a request that would result in a rule violation if the request were approved and fulfilled. This setting is applicable only if user access or segregation of duties rules are implemented on the system.
- **Show indirect entitlement violations** — If indirect entitlements are enabled for a request workflow that you use to process change requests, this setting lets you specify that the system generates a violation for the role but also for the source of the indirect entitlements in a role, those provided by an application role belonging to the role for example. By default, the option is disabled, which means that the system provides violation information only about the entitlements in a role that would violate a rule if it were granted. This setting is applicable only if user access or segregation of duties rules are implemented on the system.

  Note: *See Chapter 4, "Rules," on page 129 in the User Tasks Guide for information on rules and rule violations. See "Configuring Workflow Properties" on page 250 in the Administration Guide for information on how to enable indirect entitlements for request workflows.*
- **Request Grouping**:
  - Select **All Changes in 1 Request** to consolidate request items for multiple users into a single change request.
  - Select **Changes by User** to create change requests for each user.

Adding Additional Information Elements to a Request Submission Form

You can add a variety of information solicitation elements (fields, menus, selection buttons, and so on) to a request submission form. This enables you to configure forms that enable (and in some cases, require) requestors to provide information helpful to or required by request approvers and fulfillers to make informed decisions on how to process requests. You can specify that the fields appear in all submission forms, or you can conditionalize which fields appear based on various criteria: who is making the request, what type of request, what access is being requested, and so on.

The elements you add from the context of the Submissions tab interface appear on all request submission forms. Those added and removed from the context of an object, a particular application or business unit for example, apply only to that object. The procedure for adding and removing fields is identical for both contexts. This section describes how to configure fields from the Submissions tab context.

See the following sections for information on customizing fields for different object types:

- "Customize Submission Form Information for a Role Set" on page 57 in the *Business Role Manager Guide*.
- "Manage Additional Information Questions on a Request Submission Form for an Application" on page 177 in the *Administrators Guide*
- "Customize a Submission Form for a Business Unit" on page 162 in the *Administrators Guide*

- "Manage Additional Information Questions on a Request Submission Form for a Directory" on page 194 in the *Administrators Guide*
- "Customize a Submission Form for a Data Resource Set" on page 32 in the *Data Governance Guide*

To configure additional information fields:

1. Click the **New** button in the Additional Information section.

   The New Question window appears. The General tab is selected by default.

2. Provide a name for the question in the **Variable** field. You would typically provide a variable name that indicates the type of question or question format. For example, you might name a variable for a question that prompts a requestor to provide a priority value for a request "Priority Level Question."

3. Specify whether this question is enabled (default) or disabled using the **Enabled** option. You would disable a question if you are building and testing submission forms, and you want to selectively omit a question from the submission form during the form design process. You can, of course, enable the question at any time you want to deploy it.

4. Specify whether the question requires an answer for each user in a grouped request using the **Ask Question for Each User** option. For example, a request to create accounts for multiple users might require that additional information be provided for each user in the request.

   In this case, you would select this option. Consequently request grouping would be automatically disabled, and the system would generate a change request for each user. See "Configuring Global Request Submission Form Settings" on page 57 for more information on specifying the global group request setting.

5. Select the format used for the question from the **Control Type** field. For example:

   - You would select the **Text Field**, **Text Area**, **Date Field**, **Password Field**, **Reset Shared Passwords**, or **Number Field** type to enable requestors to enter a response in a field to a question on the submission form.
   - You would select the **Attachments** type to enable the requestor to attach one or more files to the request or the **Attachments on Request** type to enable requestors, approvers, and fulfillers to attach files to the request.
   - You would select the **Provisioning Command (Non-Visual)** type to enable execution of a command by the Access Fulfillment Express (AFX). This is applicable only if AFX in enabled.
   - You would select the **User Picker** or **Group Picker** to enable requestors to select users or groups, respectively.
   - You would select a **Drop-down** or **Radio Button** type to enable requestors to answer questions by choosing an option from a set of options.
   - You would select a **Static Text** type if you simply want to provide some information in HTML on the submission form, which could include hyperlinks and references to graphics. For example, you could use this type to state company guidelines for requesting access on a submission form and display your company logo.

   You must configure settings for the particular question format type you selected. See "Question Type Configurations" on page 60 for details.

6. Enter the question you want to appear on the submission form in the **Question** field.
7. (Optional) Enter tooltip text in the **Tooltip** field. The requestor can display the tooltip on the submission form by placing the cursor over the question.
8. (Optional) Select **Required** if requestors must answer the question on the submission form to complete the request.
9. (Optional) Specify one or more conditions for the question. A condition defines the circumstances under which a question appears on a submission form. See "Conditionalizing Questions" on page 61 for details.

Question Type Configurations

This section describes the settings you must specify for all except the Text, Static Text, and Text Area submission question types, which require you to enter text only. The New Question window displays a brief description of the purpose of each question type

- Attachments
  - Hide if empty: If selected, the Attachment field is not displayed on the request once the request has been submitted for approval.
  - Supports versions: If selected, the request stores multiple attachment versions.
  - Supports multiple files: If selected, the requestor can attach more than one file.
  - Valid extensions (comma separated): Specify that only files of a certain type (.docx, .png, and so on) can be attached. If no extensions are entered, any file type can be attached.
- Attachments on Request
  - Hide if empty: If selected, the Attachment field is not displayed on the request once the request has been submitted for approval.

  Note: *See "Specifying Access Request Settings" on page 18 for information on configuring attachment on request settings.*
- Checkbox
  - Default Value: If selected, the checkbox is selected on the submission form, which confirms the On Value setting.
  - On Value: True by default.
  - Off Value: Off by default.
- Date
  - Show Time: If selected, a timestamp is included with the date entered.
  - Allow Past Dates: If selected, the requestor can enter any date preceding the current date.
  - Allow Future Dates: If selected, the requestor can enter any date following the current date.
- Drop Down
  - Value: Stored value of an answer to the question. For example, for a "Yes" answer you could assign a value of "Y."

  - Display: An answer to the question displayed in the drop down list to the requestor, typically "Yes" or "No" or "True" or "False."
- Group Picker
  - Value: Stored value of an answer to the question, the group selected, group Name, or ID.
- Number
  - Minimum Value: The minimum number value that the requestor can enter.
  - Maximum Value: The maximum number value that the requestor can enter.
- Password
  - Validation URI: A URI called to validate the password.
  - Use Field Value For Request: Specifies whether the answer is included in the Notes or Description field of the generate change request.
  - Password Generator URI: A URI called to generate the password.
- Provisioning Command (Non Visual)
  - Business Source: The endpoint where AFX executes the command.
  - Available Commands: The command you want executed.
- Radio Buttons
  - Value: Stored value of an answer to the question. For example, for a "Yes" answer you could assign a value of "Y."
  - Display: An answer to the question provided by selection of a radio button by the requestor, typically "Yes" or "No" or "True" or "False."
- Reset Shared Password
  - Default Value: If selected, the Reset Shared Password checkbox is selected on the submission form, which confirms the On Value setting.
  - On Value: True by default.
  - Off Value: Off by default.
- User Picker
  - Value: Stored value of an answer to the question, the user selected, user Name, or ID.

Conditionalizing Questions

A condition limits display of a question on a submission to requests that meet particular criteria. For example, you may want a particular question to appear to a subset of requestors or for a subset of applications in your organization. You can apply any number of conditions to a question, and you can edit and delete conditions as required to meet your request submission requirements.

Important: *When configuring multiple conditions for an information variable, keep in mind that only one condition has to be met for the information prompt to appear on the submission form. All criteria within a condition, however, must be met for the condition*

To create a condition:

1. Click the **Display** tab in the New Question window.
2. Click **New Condition**.

   A list of condition options appears.
3. Provide a name for the condition in the **Description** field. You would typically provide a name that summarizes the condition to make managing conditions easier for other administrators.
4. Select one or more options and configure option settings.

   For example, if you wanted the additional information variable to appear only on submission forms for requests by "John Smith" and only when he requests access or changes in access for members of the "Accounting" department to the "Cost Control" application you would do the following:

   a. Select **Requestor**, and then select John Smith

   b. Select **Contains user changes**, and select Department=Accounting.

   c. Select **Contains application changes**, and then select Cost Control.
5. Click **Done** to save the condition to the information variable. All criteria specified in the condition must be met for the information prompt to appear on the submission form.

Managing Submission Variables

This section describes how to view variables created in the system and edit and delete variables.

To access variables:

1. Click the **Requests** menu and select **Workflows**.
2. Click **Submission**.

   The Submission settings page appears. The Additional Information section lists variables defined in the system.

View Variables

You can choose between two views of variables in the system:

- **Common Fields** — Displays variables that are available for inclusion in all requests (as specified by any conditions set for the variables), but not those created from the context of an object (application, business unit, data resource set, directory).
- **All Fields** — Displays all variables created in the system, including those created from the context of an object.

Order the Sequence of Variables on a Submission Form

Use the arrow icons under the **Order** column to specify the order in which information fields are listed in the request submission form.

Edit Variables and Variable Conditions

You can edit all settings for all variables, including those created from the context of an object.

To edit a variable:

1. Click the **Edit** button for the variable you want to edit.
2. Complete edits under the General tab, and then click **OK**.

To edit a condition:

1. Click the **Edit** button for the variable with the condition you want to edit.
2. Click the **Conditions** tab.
3. Click name of the condition you want to edit.
4. Complete edits, and then click **DONE**.

Delete Variables and Variable Conditions

You can delete variables you no longer require, including those created from the context of an object.

To delete a variable:

1. Select the variable you want to delete (or select multiple variables).
2. Click **Delete**.

To delete a condition for a variable:

1. Select the variable with the condition you want to delete.
2. Click **Edit**.
3. Click the **Conditions** tab.
4. Click delete icon (trashcan) for the condition you want to delete, and then click **OK**.

Localize Variables

You can localize the additional information text displayed on a request submission form by clicking the **Click here for more information...** hyperlink in the Additional Information section and following the instructions that appear.

Chapter 8: Creating and Managing Change Request Activity Monitoring Policies

Content

About Monitoring Policies

A monitoring policy defines a view of change request approvals or fulfillment activities available to a particular set of users. Monitoring policies enable you to define views that are significant to personnel in your organization who want to track the progress of approvals and activities assigned to particular users. A monitoring policy can also specify that the users to whom the policy applies can do the folloiwng:

- View activities only.
- Complete an approval or fulfillment activity.
- Reassign an activity to themselves to other users.

Once you create monitoring policies, the users to which they apply are able to access the views of the approvals and activities defined by the monitoring policies from the **Requests** menu on the RSA IMG home page.

Note: *"Monitoring Approvals and Activities Specified by Monitoring Policies" on page 24 in the User Tasks Guide describes how users can access and work with the approvals and activities they have been granted monitoring access by monitoring policies.*

Creating a Monitoring Policy

When you create a monitoring policy, you specify who the policy applies to and what approval or activity items are provided in the view the policy defines.

To create a monitoring policy:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Monitoring Policies**.
3. Click **New**.

   The Create Monitoring Policy window appears.

4. Configure the following settings:

   - **Monitoring Policy Name** — Provide a name for the policy. This is an internally saved name, not the name displayed to users who access the view defined by this policy.
   - **Display Name** — Provide the name that users select to invoke the view defined by this policy. Under **Requests -> Approvals**, for example, if this view applies to the user accessing the Approvals list the user is able to invoke that view from the list using this display name.
   - **Type** — Choose the monitoring policy type: **Approval** for a monitoring policy designed to provide a view of approvals, or **Activity** for a monitoring policy designed to provide a view of fulfillment activities.
   - **Enabled** — Select to enable the policy. Deselect to take the policy out of service.

- **Applies to Users** — Specify who this policy applies to. If, for example, you wanted this policy to apply to members of the "Accounting" department who are also members of the "Management" group you would create a filter like this:

  "Department=Accounting ALL in Group=Management"

  All users who meet this criteria can access the view defined by this policy.

- **Work Items Matching** — Specify the attribute value associated with the work items you want tracked by the users for whom this monitoring policy is designed. You can specify attributes pertaining to the work item assignee, the work item requestor, and the items included in the change request. If, for example, you wanted this policy to apply to all work items assigned to users who work for a particular supervisor ("The Boss" for example) or who also share a particular job location ("Boston" for example) you would create a filter like this:

  "Assignee Supervisor=The Boss ANY Assignee Location=Boston"

  Any work items that meet this criteria can be tracked by the users to which the this policy applies.

  You can also specify work item criteria based on configuration settings for action nodes in approval and fulfillment activity workflows that generate the work items:

  - The "Tag" attribute lets you include work items covered by this monitoring policy that are generated by any number of workflows with action nodes that have a particular Tag value. For example, if you wanted this monitoring policy to cover all work items generated by one or more approval workflows, fulfillment workflows, or any combination of the two you would select the value of the Tag attribute specified for their action nodes. See "Create Workflow Tags Used for Monitoring Policies" on page 258 in the *Administrators Guide* for more information on configuring Tag values for work items generated by approval and fulfillment workflows.

  - The "Priority" attribute lets you include work items covered by this monitoring policy that are generated by any number of workflows with action nodes that have a particular priority level. For example, if you wanted this monitoring policy to cover all work items generated by one or more approval workflows, fulfillment workflows, or any combination of the two you would select the priority level value specified for their action nodes. See "Specify a Priority Level for Work Items" on page 259 in the *Administrators Guide* for more information on specifying a priority level for work items generated by approval and fulfillment workflows.

  - The "Due Date" attribute lets you lets you include work items covered by this monitoring policy by any number of workflows with action nodes that have a due date that occurs on, before, or after the date you specify. For example, if you wanted this monitoring policy to cover all work items with a due date before the current date you would specify that date. See "Configure Work Item Due Date and Escalation Properties" on page 262 in the *Administrators Guide* for more information on specifying work item due dates generated by approval and fulfillment workflows.

- **Include work items not assigned to the current user** — Select this option if you want to enable monitoring policy members to be able to perform the approvals or update the fulfillment activities in their views.

- **Allowed to reassign work items** — Select one of the following options that monitoring policy members can perform in their views:
  - **Self assign**: Allows monitoring policy members to assign work items to themselves.
  - **User can reassign to the following users**: Allows monitoring policy members to assign work items to the users you specify.
  - **User can reassign to users with the following attributes**: Allows monitoring policy members to assign work items to only those users who share a common attribute value.
- **Allowed to change work item due dates** — Select this option to specify whether monitoring policy members can change the due dates for work items. This allows members to extend or reduce the amount of time a change request approver or fulfiller has to complete his or her tasks.
- **Allowed to change work item priorities** — Select this option to specify whether monitoring policy members can change the priority level for work items. This allows members to elevate or lessen the priority of a work item. See "Creating and Managing Request Approval and Activity Priorities" on page 272 in the *Administrators Guide* for more information on priorities.

5. Click **OK**.

   The policy takes effect, and the view of approvals or activities defined by it is available to the users to whom it applies.

Editing or Deleting a Monitoring Policy

You can edit monitoring policies as required and delete policies you no longer require.

To edit or delete a monitoring policy:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Monitoring Policies**.
3. Select the monitoring policy you want to edit or delete, and then:
   - Click **Edit** to modify the monitoring policy. The Edit Monitoring Policy window appears. Proceed as follows:
     a. Modify settings as required. See "Creating a Monitoring Policy" on page 66 for information on monitoring policy settings.
     b. Click **OK**.
   - Click **Delete** to remove the monitoring policy from the system, and then click **OK** in the confirmation window to complete the deletion.

Chapter 9: Managing Account Password Reset Implementation

Content

About Managing Account Password Reset Features

This chapter describes how to manage the following user account password reset features provided by RSA IMG and the Access Request Manager module:

- **How to Setup the System to Support External Password Reset Capabilities** — You must complete a number of prerequisite configuration tasks in RSA IMG before users are able to request a login account password reset from the RSA IMG login window and from a Windows desktop.
- **Password Management Settings** — These settings let you enable and disable password synchronization group functionality and configure the external password reset URL. The URL specifies where the desktop password reset component installation on Windows retrieves the challenge questions from a user must answer to reset his or her RSA IMG password.
- **Password Policies** — A password policy defines the password requirements (length, format, expiration, and frequency of change) for password reset requests. You can associate a policy with multiple business sources, and you can create unique policies for different types of business sources in cases, for example, where you require a more, or less, stringent password policy for the user accounts of a particular business resource.
- **Password Synchronization Groups** — A password synchronization group consists of a set of business sources that are associated with the same password policy. When a user requests that his or her password be reset for one account, the system generates additional request items to reset the passwords for the user's other accounts to the business sources in the group.

  You can create multiple synchronization groups that each define a varying scope of synchronization appropriate for the business sources in the groups. For example, you may only want synchronization to occur for a user's accounts for some business sources at a particular point in time and then all of the user's accounts at another. Once you have defined a group, you can manage synchronization in any way that meets your organization's security standards.
- **RSA IMG Login Account Password Reset Challenge Questions** — You can specify the security questions users must answer to get a new password when they have forgotten their passwords. All users in the system are required to register their answers after their identity records are collected into RSA IMG. For example, user "Mark James" is collected into the system. The system then sends email to Mark that notifies him to register his answers to the challenge questions.

Set Up the System to Support External Password Reset Requests

Important: *User password reset capability is available only when the Password Management system setting is enabled. See "Specifying System Settings" on page 36 in the Administrators Guide for more information. See "Managing System Security" on page 47 in the Administrators Guide for information on how to specify login attempt and password reset restriction settings. Consult your RSA IMG administrator if you have any questions about password reset requirements and procedures discussed in this section.*

You must complete all prerequisite tasks listed in this section to enable users the ability to request authentication source account password reset requests.

Prerequisites:

- The **Password Management** system setting must be enabled. See "Specifying System Settings" on page 36 in the *Administrators Guide* for more information. Also, See "Managing System Security" on page 47 in the *Administrators Guide* for information on how to specify login attempt and password reset restriction settings.
- To expose the external RSA IMG password reset form and challenge questions, you must specify the RSA IMG host that provides those components. See "Configuring the External Password Reset URL" on page 72 for more information.
- The business source that includes the login account for which a password reset is requested must include the account collector that collects accounts from the login authentication source. If the authentication source type is an identity collector, the business source that includes it must also have an account collector that collects the user accounts.
- A password policy must be associated with the business source that serves as the authentication source for your RSA IMG login account. See "Creating and Managing Account Password Policies" on page 72 for more information.
- Users must also have "enrolled" in the password reset system by setting up challenge (or security) questions before they attempt to reset their RSA IMG login passwords. See "How to Enroll Your Challenge Question Responses" on page 23 in the *Administrators Guide* for more information.

Configuring Password Management Settings

This section describes how to enable the password synchronization group feature and specify the RSA IMG host URL required for external password reset requests.

Enable and Disable Password Synchronization

By default, the system's ability to initiate password synchronization operations is disabled. You must explicitly enable the password synchronization feature if you want to create a password synchronization group and you want the system to initiate password synchronization operations. If you disable the feature, the system retains the password synchronization groups that have been created, but again, the system will not initiate operations defined by those groups until the feature is enabled.

To enable the password synchronization group feature:

1. Click the **Requests** menu and select **Password Management**.

   The Password Management Settings tab opens by default.

2. Select the **On** option for Password Synchronization.

   See "Creating and Managing Account Password Synchronization Groups" on page 76 for more information.

Configuring the External Password Reset URL

Note: *The external password reset installation package (AveksaKiosk-<platform>.zip) for Windows 32-bit and 64-bit platforms is available from SecurCare Online. It includes installation components and documentation that describes how to install and invoke an RSA IMG "password reset" form used to request a self-service password change. You are not required to specify a URL if external password reset capabilities are not implemented.*

The external password reset URL specifies the RSA IMG host from which you want the external password reset component on a Windows system to retrieve challenge questions for the requestor who is requesting an account password change to an authentication source. The host would typically be the one the user accesses via his or her authentication source credentials.

To configure the URL:

1. Click the **Requests** menu and select **Password Management**.

   The Password Management Settings tab opens by default.

2. Click **Edit**, and then enter the URL in the **External Password Reset** URL box.
3. Click **OK**.

Creating and Managing Account Password Policies

RSA IMG allows users to request resets of their passwords to the accounts they have to business source entitlements. Because accounts provide access to sensitive data in your organization, maintaining password security is crucial to achieving your organization's overall access security goals. A password policy specifies the quality standard for password reset requests for business source accounts. You can tailor different password policies for different business sources, or you can specify a default password policy for all business sources. Some business sources may require the most stringent password policies, while others may require less.

Specifically, a password policy enforces:

- Password strength — Minimum and maximum password length and alphanumeric character requirements and restrictions.
- Password validation — Whether a user's first or last name or his or her user ID can be included in a password.
- Password history — The number of passwords that have been previously reset that cannot be re-used in a password reset and the minimum duration before subsequent password resets can be requested.
- Password expiration — The number of days before an account password automatically expires and the number of days before the expiration the user who has the account is notified of the password expiration by the system.

Password policies also apply to business sources that are designated as authentication sources for RSA IMG user logins. In the event that a user forgets his or her login password and requests a login password reset, he or she is required to submit a new password that meets the quality standard specified by the policy associated with the authentication business source. The user in this case is also required to provide answers to challenge (or security) questions to authenticate that he or she is a valid RSA IMG user. See "Managing Login Account Password Reset Challenge Questions" on page 78 for more information.

Create a Password Policy

You can create as many password policies as you require for your business sources. You can designate a default policy for all business sources or you can designate different policies for different business sources. Once you have created a password policy and associated it with a set of business sources, you can include the business sources in a password synchronization group to support batch password resets. See "Creating and Managing Account Password Synchronization Groups" on page 76 for more information.

RSA provides two policies: the "Basic Password Policy" and the "Secure Password Policy." The basic policy is not configured (gives you a blank slate to work with); the secure policy is (provides a sample of a stringent policy). You can modify and deploy these policies to address your requirements or use them as templates to create new policies.

To create a password policy:

1. Click the **Requests** menu and select **Password Management**.
2. Click **Password Policies.**

   The Password Policies window appears.
3. Click **New**.

   The Create Password Policy window appears.
4. Specify how you want to create the policy:
   - Create a policy from scratch.
   - Create a policy from another policy by selecting the policy (the Secure Password Policy for example) you want to use as a template.
5. Click **Next**.
6. Configure the policy:
   - **Password Policy Name** — Provide a name that indicates the policy's purpose. If, for example, the policy is intended for the "Source Control" application, you could name it "Source Control Password Policy." Or if you intend to use this policy as a default policy for all business sources, you could name it "Default Password Policy."
   - **Default Policy for All Business Sources** — Specify whether this policy is the default policy for all business sources. Only one policy can be designated as a default policy. You can override the default for any business source, and business source owners can choose another policy as required.
   - **Password Strength** — Password strength is the measure of how difficult the password would be for a hacker to guess. Specify any number of alphanumeric character requirements for a password. For example, if you require that passwords must include between six and eight characters, begin with a letter and include one numeric character, and prohibit hyphens or asterisks you would configure these settings:
     - Minimum number of characters: 6
     - Maximum number of characters: 8
     - Minimum number of numeric characters: 1

- Disallowed characters: * -
- Require password to start with an alphabetic character: Enable

- **Password Validation** — Specify whether first names, last names, login IDs, and any portion of a user email address are prohibited from inclusion in passwords. When validation restrictions are enabled a password reset requestor, Joe Brown for example, would not be allowed to enter "joe" (joe1234) or "brown" (brownABCD) or his login ID or any portion of his email address as part of the new password.
- **Password History** — Specify the minimum age for a password before another password reset can be requested (a value of 2, for example, means that a user cannot request another password within two days of the last reset) and the number of previous passwords that cannot be used for password resets (a value of 3, for example, means that a user cannot request a password reset using any of his or her three previous passwords).
- **Password Expiration** — Specify the number of days a password is valid before it automatically expires and the number of days before it expires the system sends expiration notification email to the user whose password is about to expire.

7. Click **Finish**.

   You can now associate the policy to one or more business sources.

Associate a Password Policy with a Business Source

When you associate a password policy with a business source, that policy specifies the password requirements for password resets for accounts to the business source. Business source owners can override policy associations you specify with those they consider better meet their requirements. Associating a policy to a business source supplants any default policy association specified in a password policy definition.

Important: *You must associate a password policy with the business sources that serve as authentication sources for users who log into the system to enable those users to request an RSA IMG login password reset in the event they forget their passwords.*

To associate a password policy with one or more business sources:

1. Click the **Requests** menu and select **Password Management**.
2. Click **Password Policies.**

   The Password Policies window appears.
3. Click the name of the name of the policy you want to associate with a business source.

   A details view of the policy appears. The Business Sources Using This Policy section indicates which business sources have the password policy associated with them.
4. Click **Choose Business Sources**.

   A list of business sources appears.
5. Select one or more business sources, and then click **OK**.

   The policy association overrides any previous association for the business sources and is in effect for all account password reset requests for the business sources.

To associate a password policy to a business source from the context of a business source:

1. Click the **Resources** menu and select the business source type, **Applications** or **Directories**.
2. Click the name of the business source.

   The details view of the business source appears.
3. Click the **Password Policy** tab.
4. Click **Choose Password Policy**.
5. Select a policy, and then click **OK**.

   The password policy association overrides any previous association for the business source and is in effect for all for business source account password reset requests.

Edit or Delete a Password Policy

Important: *Edit or delete policies with caution. Either action on a policy affects all of the business sources that are associated with the policy.*

You can modify all password policy settings. The changes take effect immediately after you complete the editing session. You can also delete policies you no longer require. If you are a user with system administrator privileges, you can also edit a policy from the context of any business source to which it is associated, but you cannot delete a policy from the context of a business source.

To edit or delete a password policy:

1. Click the **Requests** menu and select **Password Management**.
2. Click **Password Policies.**

   The Password Policies window appears.
3. Edit or delete a policy:
   - Edit a policy:
     a. Click the name of the name of the policy you want to modify.

        A details view of the policy appears.

     b. Click **Edit**.

     c. Modify settings as required, and then click **OK**. See "Create a Password Policy" on page 73 for information about the policy settings.
   - Delete a policy:
     a. Select the policy you want to delete.

     b. Click **Delete**, and then click **OK** in the confirmation window to complete the deletion.

To edit a policy from the context of a business source:

1. Click the **Resources** menu and select the business source type, **Applications** or **Directories**.
2. Click the name of the business source associated with the policy.

   The details view of the business source appears.

3. Click the **Password Policy** tab.
4. Click **Edit**.

   A details view of the policy appears

5. Modify settings as required, and then click **OK**. See "Create a Password Policy" on page 73 for information about the policy settings.

Creating and Managing Account Password Synchronization Groups

Important: *Use synchronized password groups for password reset requests with caution. Anyone in your organization who gains knowledge of a synchronized account password for a user can gain access to all of the user's accounts that share the password.*

An account password synchronization group expedites the process of setting a single common password for accounts a user has to multiple business sources that are associated with the same password policy. A synchronization group includes those business sources to which users have accounts. An account password reset request is the catalyst for the system to automatically generate additional request items for password resets for the other accounts users have to the business sources in the synchronization group.

At least one business source in a synchronization group must be designated as a "synchronization trigger" source. That designation means that when a request is generated to reset a user's account password for a business source trigger, the system generates additional request items to reset the user's account password for each of the other business sources in the group with a common password.

For example:

User "Mark James" has accounts for the following business sources in a synchronization group: A, B, C, and D. He wants to reset his account passwords to the business sources to a single common password.

1. Mark requests a password reset for his account to business source B.
2. RSA IMG generates a request to reset Mark's password for each account he has to the business sources.

   Business source B is designated in the synchronization group as a "synchronization trigger." That means that when Mark requested the account password reset, the system automatically generated additional request items to reset the passwords for the accounts Mark has to the other business sources in the group (A, C, and D) with the same password specified in the reset request for business source B.

3. The change request with the four reset items is processed according to the approval and fulfillment workflows associated with the Default Reset Password Form or a similar form designed for account password resets.

   Note: *For usage information for the "SynchronizePassword" sub-command for the web services "createChangeRequest" command, see the web services user interface.*

4. Mark's new password for his four accounts is posted under his **My Passwords** option. See "View Your New Password" on page 109 for more information.

Create an Account Password Synchronization Group

Note: *The* ***Password Synchronization*** *setting must be enabled to create and manage password synchronization groups. See**"Enable and Disable Password Synchronization" on page 71* *for more information.*

You can create as many different synchronization groups as you require to manage the password reset synchronization requirements in your organization.

To create the synchronization group:

1. Click the **Requests** menu and select **Password Management**.
2. Click **Password Synchronization**.

   A list of password synchronization groups that have been created appears along with the number of business sources each group is associated with. The system does not provide default synchronization groups.
3. Click **New**.
4. Configure the synchronization group:
   - Name — Provide a unique name, typically one that indicates the group's purpose. For example, you might want to name for a group that includes various "Accounting" applications as "Accounting Apps Password Reset Synchronization Group."
   - Description — (Optional) Provide a description that informs other access compliance stakeholders about the group's purpose.
   - Password Policy — Select the policy that is associated with the business sources that you want in the group. The Associated Business Sources table lists all business sources associated with the password policy you specify.
   - Associated Business Sources:
     - Select *only* those business sources that you want included in the group. For example, a password policy can be associated with numerous business sources, but you may only want to synchronize account passwords for a select sub-set of those business sources. As your requirements change you can revise your selections.
     - Select the **Is Source** option *only* for those business sources in the group for which an account password reset request triggers synchronization of account passwords for other selected business sources in the group. The option designates the business source as the catalyst for password synchronization when a user requests a password reset for an account for the business source.

       You must select this option for at least one business source. For example, assume that business sources A, B, C, and D are members of the group. Assume also that you select the Is Source option for A and C. Any account password reset request for A or C will trigger synchronization of the account passwords for all of the other business sources in the group.
5. Click **OK**.

   The synchronization specifications take effect immediately.

Edit or Delete a Password Synchronization Group

1. Click the **Requests** menu and select **Password Management**.
2. Click **Password Synchronization**.

   A list of password synchronization groups that have been created appears along with the number of business sources each group is associated with.
3. Select the synchronization group you want to edit or delete.
4. Edit or delete a synchronization group:
   - Edit a synchronization group:
     a. Click the name of the name of the synchronization group you want to modify.

        A details view of the synchronization group appears.
     b. Click **Edit**.
     c. Modify settings as required, and then click **OK**. See "Create an Account Password Synchronization Group" on page 77 for information about synchronization group settings.
   - Delete a synchronization group:
     a. Select the synchronization group (or multiple synchronization groups) you want to delete.
     b. Click **Delete**, and then click **OK** in the confirmation window to complete the deletion.

Managing Login Account Password Reset Challenge Questions

You must specify that one or more of the system-provided challenge (or security) questions are posed to and answered by users when they request password resets for their RSA IMG login accounts in the event that they forget their login passwords. Users must provide the answers to all of the questions in advance under their **Users > My Passwords > Challenge Questions** tab.

System-generated email notifies all users that they must complete answers to their challenge questions. The system continues to notify those users who have failed to do so after the first notification. Users must then provide the answers to one or more of their challenge questions when they request a password reset after a failed RSA IMG login attempt.

Note: *See "Managing System Security" on page 47 for information on how to specify a restriction on the number of password resets users are allowed to attempt.*

To manage challenge question implementation:

- Specify the number of challenge questions (all are enabled by default) that are available to users:

  Disable the challenge questions you do not want available to users by clicking **Disable** under the Action column for those questions.
- Specify the number of challenge questions and answers that you want users to set up and the minimum number of questions a user must answer to reset their passwords:
  1. Click the **Requests** menu and select **Password Management**.

2. Click **Challenge Questions**.

   By default, all challenge questions are listed. You can choose to view only enabled or disabled challenge questions or all questions.

3. Click **Edit Settings**.

   The Configure Challenge Questions dialog box appears.

4. Configure settings:

   - **Number of question/response pairs required to provide when enrolling** — Enter the number of system-provided and enabled questions you want the user to provide answers for.
   - **Number of questions required to answer successfully to reset an account password** — Enter the minimum number of questions from the set of total questions a user must answer correctly to satisfy the challenge phase of the RSA IMG account password reset request process.

5. Click **OK**.

   The challenge questions go into effect immediately for all RSA IMG login account password reset requests.

Chapter 10: Set Up the System for New User Registration Requests

Content

Set Up the Directory Where New Users Are Created

This section describes how to prepare RSA IMG for registering (or on-boarding) new users into an Active Directory (AD) authentication source used to authenticate users who log on to RSA IMG.

Complete the following set up tasks:

1. If you have not already on-boarded an Active Directory (AD) that you use as a user authentication source in RSA IMG, create the directory using the Create Active Directory wizard. The wizard also allows you to create an AD identity collector, an AD account collector, and an AFX AD connector for the directory. All of these elements are required to support register new user requests. See "Creating an Active Directory (AD) Directory with the Wizard" on page 189 in the *Administrators Guide* for more information.

   The AD connector must include an enabled "Create an Account on a AD server" command and parameters. See the *Access Fulfillment Express Guide* for more information.

2. If you have not already created the AD authentication source, create it using the account collector as the authentication type for the AD directory. See "Creating a New Authentication Source" on page 42 in the *Administrators Guide* for more information.

3. Verify that you have all of the required components in RSA IMG required to support register new user requests:

   - The directory should be listed under **Directories**.
   - The **Collectors** tab in the directory's details view should list the AD identity collector and the AD account collector.
   - The **AFX Connector Binding** tab in the directory's details view should list should list the AFX AD connector.
   - The Fulfillment section under the **Requests** tab in the directory's details view should indicate that the Default AFX Workflow or a variation of it is associated with the directory. Ensure that the connector is deployed. See the *Access Fulfillment Express Guide* for more information.

Optional Recommended Setup Tasks

You should complete the following setup tasks to fully leverage the new user creation capabilities provided by RSA IMG

- Associate a password policy with the directory you created. The request form or web services command to on-board a new user can be configured to initiate auto-generation of a password for the new user to the directory. The system requires that a password policy is associated with the directory to complete this task. See "Creating and Managing Account Password Policies" on page 72 for more information.
- Create a naming policy and associate it with the directory. A naming policy defines how a user's first and last name entered into the request form or web services command to create a new user is transformed into a name for a user ID, account name, email address prefix, or any other attribute specified in the naming policy that is compatible for the AD directory. See "Creating and Managing Naming Policies" on page 83 for more information.

Creating and Managing Naming Policies

Note: *You must have system administrator privileges to create and manage naming policies.*

A naming policy is designed to be integrated into the request process to create a new user. It defines how RSA IMG renders a unique user name, email address prefix, or account ID for example from values entered by a requestor into a "Register User" form or in a "createChangeRequest" web services command when he or she initiates a request to create a new user record in an Active Directory (AD) source.

Important: *A naming policy construes a unique name as one that has not been collected into RSA IMG at the time the register user request is generated. It also does not consider names in pending requests.*

A fully configured naming policy includes the following elements:

- General metadata about the policy that differentiates it from other naming policies you create.
- A JavaScript transform that converts a name entered into a form or a web services command into a name consistent with the format rules for names in the AD directory where a requestor wants to create a new user. For example, one of the three transforms that can be specified in a naming policy converts "Jane Doe" into "JaneD." The naming policy designer must know in advance which transform to use in the policy.
- A set of name suffix settings that define how a unique name is rendered. There may be, for example, multiple variations of the base name "JaneD" in RSA IMG. So if "JaneD," "JaneD1," and "JaneD2" already exist in the system, it appends a suffix to the transformed base name to render a unique user name, "JaneD3" for example.
- An attribute mapping specification that identifies the user attribute for which the system renders the unique name. For example, you may want a naming policy to specify how a user ID is generated from the name a requestor enters into the request. In this case you would map the policy to the "User ID" attribute. The systems checks the existing user ID attributes to determine if the name you want to generate is unique or if the suffix must be incremented.

Once a naming policy has been created, it can be implemented in the request process to create a new user as follows:

- The policy is associated with an AD directory in RSA IMG. This directory must serve as the authentication source for the user who is going to be created. The directory has associated with it the AFX connector that ultimately adds the new user to directory and the identity collector and the account collector that ultimately collects the new user's identity and account information, respectively, once the user has been created.

  See "Associate a Naming Policy with a Directory" on page 86 for more information.

- The policy is specified in the Register User form used to request creation of the new user.

  See "Configuring the Register User Form" on page 87 for more information.

  Note: *A form is not required if your organization's security policy mandates that requests to on-board a new user should only be initiated via web services.*

Create a Naming Policy

You can create as many naming policies as you require to auto-generate names for users you want to create in your AD user and account data sources.

To create a naming policy:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Naming Policies**.

   A list of naming policies appears along with the number of business sources associated with each policy.

3. Click **New**.

   The Create Naming Policy window appears.

4. Specify how you want to create the policy:

   - Create a policy from scratch. (The system does not provide any default naming policies. Therefore, you must select this option for the first policy you create.)
   - Create a policy from another policy by selecting the policy you want to use as a template.

5. Click **Next**.

6. Configure General Naming Policy Setup settings:

   - **Naming policy name**: Provide a name that indicates the policy's purpose.
   - **Naming policy reference name**: Provide an internal reference name for the policy. The name must not include any spaces. Do not change the reference name after you have created and implemented the policy. The reference name allows you to change the naming policy name of the policy without impacting how the system looks up the policy. For example, web services looks up a naming policy by its reference name, not the policy name.
   - **Naming policy description**: Provide a description of the policy.
   - **Enforce uniqueness**: Select this option to specify that only unique names are created.

7. Select the transform used to create base names from the **Name transform to use** transform selection option. RSA IMG provides four JavaScript transforms:

Transform	What it Does

FirstName LastName 1st letter
`var OUTPUT_VALUE = getBaseName();`
`function getBaseName() {`
`  var firstName = INPUT_VALUE[0];`
`  var lastName = INPUT_VALUE[1];`
`  return firstName + lastName.substr(0, 1);`
`}`
	Transforms a name, "Jane Doe" for example, into "JaneD."

Transform	What it Does

FirstName dot LastName
`var OUTPUT_VALUE = getBaseName();`
`function getBaseName() {`
`  var firstName = INPUT_VALUE[0];`
`  var lastName = INPUT_VALUE[1];`
`  return firstName + '.' + lastName;`
`}`
	Transforms a name, "Jane Doe" for example, into "Jane.Doe."

LastName FirstName 1st letter
`var OUTPUT_VALUE = getBaseName();`
`function getBaseName() {`
`  var firstName = INPUT_VALUE[0];`
`  var lastName = INPUT_VALUE[1];`
`  return lastName + firstName.substr(0, 1);`
`}`
	Transforms a name, "Jane Doe" for example, into "DoeJ."

1st letter FirstName LastName
`var OUTPUT_VALUE = getBaseName();`
`function getBaseName() {`
`  var firstName = INPUT_VALUE[0];`
`  var lastName = INPUT_VALUE[1];`
`  return firstName.substr(0, 1) + lastName;`
`}`
	Transforms a name, "Jane Does" for example, into "JDoe."

Note: *You cannot edit the transforms, and you cannot create new transforms.*	

8. Configure the Uniqueness section settings:

   - **Allow base name if unique**: Select only if you want the first instance of a user ID name generated by a transform to not include a suffix. By default, this option is deselected, which means suffixes are appended to names. If you select this option and if the system detects an identical name already collected into the system, it appends a suffix to the name.
   - **Sequence starting number**: This setting specifies the starting number for suffixes. The default value is "1." For example, assume user ID names must be generated for three users named Jane Doe and also assume that the "FirstName LastName 1st letter" transform is in effect. In this case the following user IDs for Jane Doe are generated: "JaneD1," "JaneD2," and "JaneD3."
   - **Sequence increment value**: This setting specifies the incremental value increase for suffixes. The default value is "1." For example, assume user ID names must be generated for three users named Jane Doe and also assume that the "FirstName LastName 1st letter" transform is in effect and the increment value is "5." In this case the following user IDs for Jane Doe are generated: "JaneD1," "JaneD6," and "JaneD11."

9. Configure the Attribute Mapping setting using the **Attribute to map policy to** drop-down selection box.

   This setting is used to associate the naming policy with a system attribute (User.User_Id for example) so that the system can check in the system database, for example, whether a potential User ID generated by a transform for a new user already exists in the system.

If the User ID exists, then the system begins appending a suffix to the end of the base User ID ("JaneD" to "JaneD1" to "JaneD2" and so on for example) until a unique User ID is created.

In the case where an email address or an account name must be generated, you would map to User.Email_Address or Account.Name, respectively, to verify uniqueness of those names.

10. Click **Finish**.

    You can now implement the naming policy to support new user on-boarding.

Associate a Naming Policy with a Directory

When you associate a naming policy with a directory, that policy specifies how the user attribute information entered by a requestor into the request form used to create a new user in the directory is transformed into a unique name. A typical use case would involve a user ID, an email address prefix, or an account name. In the case where unique names would be required for all three, the directory would be required to have three naming policies associated with it, where each policy is mapped to each of the following attribute types:

- User.User_Id
- User.Email_Address
- Account.Name

When the system processes the request, it generates the names based on the naming policies associated with the directory.

To associate a naming policy with one or more directories:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Naming Policies**.

   A list of naming policies appears along with the number of directories each policy is associated with.

3. Click the name of the policy you want to associate with a directory.

   A details view of the naming policy appears. The Business Sources Using This Policy section indicates which directories have the naming policy associated with them.

4. Click **Choose Business Sources**.

   A list of directories appears.

5. Select one or more directories, and then click **OK**.

   The naming policy is in effect for all register new user requests.

To associate a naming policy to a directory from the context of a directory:

1. Click the **Resources** tab and select **Directories**.
2. Click the name of the directory.

   The details view of the directory appears.

3. Click the **Naming Policies** tab.
4. Click **Choose Naming Policies**.

5. Select one or more policies, and then click **OK**.

   The naming policy association overrides any previous association for the directory and is in effect for all requests to create a new user in the directory.

Edit or Delete a Naming Policy

Important: *Edit or delete naming policies with caution. Either action on a policy affects all of the directories that are associated with the policy.*

You can modify all naming policy settings. The changes take effect immediately after you complete the editing session. You can also delete policies you no longer require.

To edit or delete a naming policy:

1. Click the **Requests** menu and select **Configuration**.

   The Requests Configuration window appears.

2. Click **Naming Policies**.

   A list of naming policies appears along with the number of directories each policy is associated with.

3. Edit or delete a naming policy:

   - Edit a policy:

     a. Click the name of the name of the policy you want to modify.

        A details view of the policy appears.

     b. Click **Edit**.

     c. Modify settings as required, and then click **OK**. See "Create a Naming Policy" on page 84 for information about the policy settings.

   - Delete a policy:

     a. Select the policy you want to delete.

     b. Click **Delete**, and then click **OK** in the confirmation window to complete the deletion.

Configuring the Register User Form

Note: *The AFX connector designated to fulfill a register user request may, under some circumstances, be configured to fulfill the creation of a new user in an AD directory using non-standard LDAP parameters. If this is the case in your environment, your form should contain special input parameters. See "When You Must Use Special Input Parameter Values" on page 90 for more information.*

A requestor uses a register user form to request creation of a user in an AD directory. The form must be configured to accept input required to create the user. This section describes the fields you must include in the form and optional, but recommended, fields that you can include in the form. Once you have completed configuring the form, authorized users can access the form to request creation of a new user. See "Requesting Creation of a New User" on page 107 for more information.

To create the register user form:

1. Create a form of the **Register User** type. You cannot create your first register user form using any of the system-provided default forms as a template. You can, of course, create other register user forms using your original register user form as a template. See "Creating a Form" on page 28 for more information on form design topics that are referenced, but are not covered in detail, in this section.
2. Configure General Properties settings. Choose the AD directory for which this form is intended from the **Directory** link.
3. Configure fields for the form:
   - See "Required Register User Form Fields" on page 88 for more information.
   - See "Recommended Register User Form Fields" on page 89 for more information.
4. Create a request button for the register user form and make it available wherever you deem appropriate for users who are authorized to request creation of a new user in your organization. See Chapter 3, "Creating and Managing Access Request Buttons," on page 21 for more information on your options for providing users access to a form.

Required Register User Form Fields

The register user form must include the following fields:

- The form must include **First name** and **Last name** text fields that allow the requestor to enter the user's name.
- The form must include a **Register User Command (Non-Visual)** field type. This field includes the parameters AFX requires to create a new user in the AD directory (using the "Create an Account on a AD server" command).

  Note: *The parameter display names below are examples. The AFX connector that fulfills the register user requests in your environment may include different display names for the parameters and may include different parameters.*

  Parameter configuration guidelines:

  - The **Account ID** parameter must be configured with the value used for the Account ID configuration setting in the account collector for the directory, typically "sAMAccountName." Otherwise, the system cannot verify and close the register user request if it cannot identify the new user account after data collection.
  - The **Account Name, sAMAccountName, and Common Name** parameters can each be configured with the value generated by a Naming Policy Transform (Non-Visual) control type field that is included in the register user form configuration. For example, assume a Naming Policy Transform (Non-Visual) control type field named "accountTransform" is included in the form configuration. In this case you would select the following value for the parameter to which it applies:

    ${avform.accountTransform}

    Otherwise, you must create a text field in the form that prompts the requestor for a value. In some cases, requirements may dictate that provide distinct values for these fields, rather than those generated by a naming policy.

- The **Last Name** parameter in this field must be configured with the last name value for the user (that is, the name the requestor enters for the last name prompt in the register user form). For example:

  ${avform.last}

- The **First Name** parameter in this field must be configured with the first name variable for the user (that is, the name the requestor enters for the first name prompt in the register user form). For example:

  ${avform.first}

- The **Email address** parameter in this field can be configured with a value generated by a Naming Policy Transform (Non-Visual) control type field that is included in the register user form configuration. For example, assume a Naming Policy Transform (Non-Visual) control type field named "emailTransform" is included in the form configuration. In this case you would select the following email prefix value for the parameter:

  ${avform.emailTransform}

  You must also enter the email address domain name to the value, and you can optionally enter any additional characters (xyz for example) to the prefix. For example:

  xyz${avform.emailTransform}@some_domain_name

  If you do not use a value generated by a naming policy, you can simply bind this parameter to the value of another field that prompts the requestor to enter an email address.

- The **Initial password to set** parameter in this field must be configured with the following value: **${GeneratedPassword}** if you want the system to generate a password for the new user to the AD directory. The directory where you want to create a new user must be associated with a password policy. See "Associate a Password Policy with a Business Source" on page 74 for more information.

  If you do not want the system to generate a password, you can provide one. In either case, the new user is required to change his or her password the first time he or she logs into the target AD directory.

Recommended Register User Form Fields

Although you are not required to include the following fields to the register user form, RSA recommends that you do include them to leverage automated email notification and AD-compliant naming capabilities.

- If you want the system to send notification email that contains the new user's account ID and password to the new user or to anyone else authorized to receive this information, you can include a text field in the form that prompts the register user requestor to provide the intended recipient's email address.

  This text field must be configured with a variable name of **RUq_NotificationEmail**. You can also provide a default value in the field, some sample text for the email prefix and email domain name (yourOrg.com) that the requestor can overwrite in the form. For example:

  some_text@yourOrg.com

Note: *The first time the new user logs into the AD directory with this password, the user is prompted to change his or her password. Once the user is granted access to the AD domain, her or she is able to log in to RSA IMG using the account collector configured for the directory as the authentication source.*

- If you want to leverage naming policy capabilities, you can include one or more Naming Policy Transform (Non-Visual) field types for each unique name type you want the system to render. These naming policies must be associated with the directory where you want the user created. See "Creating and Managing Naming Policies" on page 83 for more information.

When You Must Use Special Input Parameter Values

An AFX connector, under some circumstances, may be configured to fulfill the creation of a new user in an AD directory using non-standard LDAP parameters. By default, the Register User Command (Non Visual) control type field maps its parameters to the standard types:

Parameter Display Names	Standard LDAP Parameters
Account Name	Account Name
sAMAccountName	sAMAccountName
Common Name	CN
Last Name	SN
First Name	givenName
Email address	mail
Initial password to set	Password

In cases where you cannot map to LDAP standard types, you can create text fields with the following variable names and then map the values gained from those fields from a requestor to the corresponding parameters in the Register User Command (Non Visual) control type field.

- **RUq_EmailAddress** — This parameter is required if the AFX connector does not use the standard "mail" LDAP parameter. Create a text field with this name and map the parameter value to the "Email Address" parameter in the Register User Command (Non Visual) control type field.
- **RUq_UserId** — This parameter is required if the AFX connector does not use the standard "sAMAccountName" LDAP parameter. Create a text field with this name and map the parameter value to the "sAMAccountName" parameter in the Register User Command (Non Visual) control type field.
- **RUq_FirstName** — This parameter is required if the AFX connector does not use the standard "givenName" LDAP parameter. Create a text field with this name and map the parameter value to the "First Name" parameter in the Register User Command (Non Visual) control type field.
- **RUq_LastName** — This parameter is required if the AFX connector does not use the standard "sn" LDAP parameter. Create a text field with this name and map the parameter value to the "Last Name" parameter in the Register User Command (Non Visual) control type field.

- **RUq_Password** — This parameter is required if the AFX connector does not use the standard "Password" LDAP parameter. Create a text field with this name and map the parameter value to the "Initial password to set" parameter in the Register User Command (Non Visual) control type field.

About Register User Notification Email

When the request is completed (fulfilled and verified in collected user and account data), the system generates a RegisterUserPasswordEvent email event. The system sends the email, which contains the new user's account ID and password, to the user designated by the RUq_NotificationEmail field in the form.

Note: *If you are using the web services command, the list of Parameters should contain a Parameter named "RUq_NotificationEmail" that has the notification email address value: value@value.com*

You can manage register user notification email in the following ways:

- Modify this event's name and description from its details page.
- Modify the contents of this email specified in the RegisterUserPasswordEvent email template.

See Chapter 17, "Managing Email Features," on page 219 in the *Administrators Guide* for information on working with email events and email templates.

About Importing and Exporting Register User Forms and Naming Policies

You can export and import register user forms and naming policies just as you can other objects in RSA IMG. The typical scenario involves developing register user form objects and other RSA IMG objects in a test environment, exporting the objects, and then importing them into a production environment. This section discusses considerations you should be aware of before you export and import register user objects.

Considerations When Exporting Register User Objects

To ensure a successful export of register user objects, take note of the following considerations

- RSA IMG will not export an encrypted parameter that is hard-coded or partially hard-coded from a register user command non-visual field.
- When you export a naming policy, the name of the base name transform and the name of the directories associated with the naming policy are exported as well. However, you can export a naming policy without its base name transform if the base transform for the policy exists on the system where the policy will be imported.

Considerations When Importing Register User Components

Consider these points before you attempt to import register user components:

- If the directory a register user form is associated with on the source system does not exist on the target system, the import of the form will fail.

- If the directory a register user form is associated with on the source system does not have an AFX connector associated with it in the target system, the import of the form will fail.
- If a register user form is exported without an encrypted parameter in a register user command (non-visual) command, the value will display "Change me" in the form after the import and you will not be allowed to save the form until you provide the value.
- If a register user form includes a naming policy transform (non-visual) field in the source system and the naming policy specified in the field does not exist on the target system, you will be required to import/create the naming policy and update the field to specify the correct naming policy.

  If the policy isn't created before the field and a new naming policy was selected in the field, you will not be able to save the field.
- When you attempt to import a naming policy, the system searches for an existing policy with the same *reference name* as the policy you intend to import:
  - If a naming policy does not exist, then the policy will be imported.
  - If the policy does exist and the overwrite option is not selected, then the import of the policy will be skipped.
  - If the policy exists and the overwrite option is selected, then the system searches for an existing policy (other than the one already found) with the same name as the policy being imported. If the system does not find any other policy with that name, then it updates the existing policy that was found in the first place. If the system finds another policy with the same reference name, the import of the policy will fail.
  - The system also looks up base name transform by its name in the policy being imported. If it cannot find the base name transform, the import of the policy will fail.
  - The system also looks up the directories associated with the policy by their names. For each directory found, the system re-establishes the association. For each missing directory, you must associate the policy with the directory manually.

Troubleshooting Register User Request Problems

This section provides information that can help you pinpoint and resolve problems you may encounter initiating a register user request and problems related to the fulfillment of the request and its verification by RSA IMG.

- If encounter a problem at any stage in the request, request fulfillment, and request validation process, make sure all components that support user registration capabilities have been set up correctly. See "Set Up the Directory Where New Users Are Created" on page 82 for more information on the following:
  - Make sure you have AD directory in RSA IMG. AD is the only supported directory for user registration.
  - Make sure the AD connector is associated with the directory, and that the connector's "Create an Account on a AD server" command is enabled.
  - Make sure the directory's AD identity collector and AD account collector are configured correctly.

- Make sure the AD directory is an authentication source.

- The fulfillment verification "watch" in RSA IMG has not closed and therefore the request has been completed even though you have verified the following:

  - The **Status** column in the change request indicates that AFX has fulfilled the request.
  - The new user and new user account have been collected into the system.

  The probable root cause of this problem is that the "Account ID" parameter in the register user form or web services command was configured with an incorrect value. The Account ID must be the parameter that is associated with the account's name or the watch will not close. Verify that the Account ID in the "Register User Command (Non-Visual)" field control matches the "Account ID: setting in the account collector for the AD directory.

- A naming policy is used in the register user form to generate a unique user ID, but AFX fails to create the user with a unique ID in the AD directory. The **Comments** icon window in the request indicates that it could not create the new user with a unique ID in the directory.

  A naming policy generates an ID that is unique in *collected* data. The AD directory may have IDs that have not yet been collected into the system. Therefore, AFX cannot create the new user ID if it is not unique in the AD directory. Do the following to resolve the problem:

  1. Run data collections to get fresh data from the AD directory.
  2. Complete any in-progress register user requests. You may have multiple new user registration requests that are in progress, and one or more of these could generate the same ID.
  3. Repeat the request.

  You should examine how the naming policy is configured. It can only be mapped to a single attribute (User.User_Id for example); the generated ID will be unique among the collected attributes in the specified directory. Examine the register user form or web services command and make sure that the correct naming policy transform is used for that attribute. For example, if the naming policy is mapped to User.User_Id, do not associate the naming policy transform field with the user's email address.

Chapter 11: Managing How Entitlements Are Requested Using Resource Profiles

Content

About Resource Profiles

A resource profile consists of a set of entitlements (granular entitlements, application roles, groups, roles, or data resources) that you do not want users to be able to request or to be included in "suggested entitlements" lists. These lists include those provided when users request access, roles suggested in role mining operations and entitlements suggested in provisioning operations. You can create resource profiles for all business sources: applications, directories, role sets, and data resource sets. By restricting the entitlements users can request access to for themselves or other users, you not only place some entitlements as "off limits" (for whatever reason) but you can also control the way the entitlements can be requested via their association with application roles, groups, and roles rather than on a per-entitlement basis.

A resource profile enables you to provide an efficient way to control how entitlements to your business source are granted to users. For example, your application may include numerous entitlements you want users to have but you do not want them to be requested on a per-entitlement basis. Instead, you may want the entitlements to be consolidated in one or more application roles and allow them to be requested instead. In this scenario, users can request access to the entitlements indirectly via requests for the application roles that include the entitlements but not to any of the particular entitlements cafeteria style.

You can elect to restrict access to all or a subset of a business source's entitlements. Resource profiles neither hinder the system's ability to collect the entitlements included in them, nor do they trigger any actions to remove the entitlements from users who have them. Entitlements can be added or removed from a resource profile at any time, which means that entitlements are instantly available when they are removed from a resource profile and instantly unavailable when added to a resource profile. Entitlements that are included as change items in change requests are not affected if the entitlements are added to a resource profile.

Note: *Except for most of the granular entitlements for the Aveksa security application, those that are implicitly granted by the system to users who have particular job roles, review and rule owners for example, all business source entitlements are available for requests and suggestions by default until you explicitly exclude them by adding them to a resource profile. See* *Chapter 6, "Managing RSA IMG Application Privileges," on page 103* *for information on Aveksa security application entitlements and application roles.*

Creating and Managing Resource Profiles

Create an resource profile to control how users are able to request access to a business source's entitlements.

To create a resource profile:

1. Access the details view of the business source for which you want to create a resource profile:
   - Application — See "Access a Details View of an Application" on page 170 in the *Administrators Guide*.
   - Directory — See "Accessing a Details View of a Directory" on page 185 in the *Administrators Guide*.
   - Role set — See "Viewing Role Set Details" on page 50 in the *Business Role Manager Guide*.

- Data resource set — See "Access a Details View of a Data Resource Set" on page 28 in the *Data Access Governance Guide*.

2. Click the **Resource Profile** tab.

   There are two options available to you:

   - Exclude all of the business source's entitlements from entitlement selection and suggested entitlement lists:

     a. Click **Edit Settings**

     b. Select **Yes** for the **Exclude Entire Application From Add Access And Suggestions** option.

     c. Click **OK**.

     The **Exclude from Add Access** table column available in the summary window for the type of business source you are working with indicates that the business source's entitlements are unavailable for requests and suggested entitlements lists.

   - Add a subset of the business source's entitlements to the resource profile.

     a. Click **Add Entitlements**.

     b. Select the entitlements you want to add to the resource profile, and then click **OK**.

     The entitlements appear in the **Individually Excluded Entitlements** table. The entitlements are unavailable for requests and suggested entitlements lists. The **Available for Requests** table column available from the **What Access** tab for a business source indicates that the entitlements are unavailable (No) for requests and suggested entitlements lists.

3. Make any adjustments to your actions as follows:

   - Use the **Remove** button for an entitlement in the table if you want to make the entitlement available again.The button label changes to **Removed**. This indicates that the entitlement is no longer excluded and is available for requests and suggested entitlements lists.

   - If, instead, during your session in the table you want to cancel the removal of the entitlement from the excluded list click the **Removed** button. It will change to **Canceled**. This indicates that you removal operation has been reverted and the entitlement remains in the excluded list.

4. Verify that excluded entitlements are unavailable for requests by using any of the following methods:

   - Check the **Available for Request** column value from the **What Access** tab to determine if the entitlements you excluded are indicated as unavailable for requests. Use the **Table Options** link to display the column if it is not displayed.

   - Perform a test an access request operation to determine whether the entitlements you excluded are absent from the Select Entitlements window.

   For entitlements you have removed from the excluded use the same methods to determine that the entitlements are available for requests: the entitlements are indicated as available for requests, and a Select Entitlements window lists the entitlements.

Chapter 12: Requesting and Changing Access

Content

About Requesting and Changing Access

By providing self-service access management and enabling supervisors and other stakeholders to request access and change access from multiple locations throughout the RSA IMG user interface, Access Request Manager eliminates obstacles that hinder expeditious granting of access to and revocation of access from your organization's resources.

When you request access, you may be presented with an interactive form that requires you to answer questions or select options before you actually request access to entitlement or changes to entitlements for yourself or others and provides helpful instructions. You may also be presented with custom access request buttons that invoke access forms or provide you with a particular view of users and entitlements. Upon submitting a request, you may be alerted that the ultimate fulfillment of the request would violate a user access or segregation of duties policy that is in effect (see "About Access Request and Decision Support Rules" on page 14 for more information). Consult your Access Request Manager administrator if you have questions about access request resources at your disposal.

Request and Change Access From Multiple Locations

Access Request Manager enables you to request access and changes to access from the following locations in RSA IMG:

- Users summary view
- User details view
- Requests menu
- Home page

Only users with system administrative privileges in RSA IMG can request access and changes to access from all of these locations. If you are a non-administrative user, your options are limited to your dashboard and any other location you may be privileged to access with the appropriate RSA application entitlements.

Note: *For the sake of simplicity and unless specified otherwise, access request and change request procedures in this chapter reference a single location for requesting access, the* ***Home*** *dashboard, that all users can access regardless of the RSA application entitlements they may or may not have. Also, request procedures in this chapter assume a request button is available for the type of request you want to initiate. Finally, the procedures in this chapter do not attempt to cover the large number of various options available to requestors if advanced custom access request forms are implemented on the system. Consult your system administrator for information about request buttons and options and form-based access requests.*

About Changing Access

You can change access in the following ways:

- Add access to yourself and other users.
- Remove access from yourself and other users.
- Change your access and the access of other users.

Important: *You can remove entitlements from users that are directly granted to those users. Therefore, the "Remove" button on a change access form appears only for those directly granted entitlements.*

About Attaching Files to Change Requests

Requests can be configured to support file attachments. All attached files are available in the change request sequence. For example, files attached to approvals are available in the change requests that generated the approvals and the activities created when the approvals are completed.

Important: *A requestor can attach files to a request when he or she initiates a change request. Only users with System Administrator or Access Request Administrator privileges can add attachments to change request approvals and activities.*

File Attachment Management:

- **Attaching a file:** Browse to the file location, select the file, and click **Upload Attachment**.
- **Viewing an attached file:** Click the name of the attached file, and then open with the appropriate program (MS Word for .doc files for example).
- **Viewing/Hiding attached file details:** Click the **Show Details/Hide Details** toggle.
- **View file version details:** The Show Details view list versions of a file if the multiple file version configuration option is enabled.
- **Delete an attached file:** From the Show Details view, select the file and click **Delete**.

For more information:

- See "Adding Fields to a Form" on page 31 for information on how to add an attachment field to a request form.
- See "Adding Additional Information Elements to a Request Submission Form" on page 58 for information on how to add an attachments field to a request submission form.
- See "Specifying Access Request Settings" on page 18 for information on settings that specify the types of files (.doc, .pdf, .png, and so on) that can be attached to a request and whether the system maintains versions of files.

Requesting Access

When you request access for yourself or other users, RSA IMG generates a change request to fulfill the request. Whether the access request is fulfilled depends on whether the request is approved by personnel designated as approvers in a change request workflow. You can view change requests you have initiated under the **Requests** menu or under the **Manage Access** dashboard on the Home page.

Note: *You may be limited in the number of users you can select when you request access for other users. Consult your access request administrator if you have questions about user selection limits.*

About Request Submission Procedure Options

For all explicit request types (those not automatically generated by RSA IMG), you may have the option to configure request settings or be required to provide additional information about your request after you specify what entitlements you want to add or remove.

For example, you may see and be able to configure the following fields:

- **Notes** — Enter commentary.
- **Attributes** — Provide values for any attributes configured for requests. Consult your RSA IMG administrator for questions about attributes for requests.
- **Fulfillment Date** — Specify a date on which you want the entitlement addition/removal fulfilled in the data source. You would specify a fulfillment day to delay the entitlement addition/removal.
- **Revocation Date** — Specify a date upon which RSA IMG will automatically generate a change request to revoke the entitlement add in this request. You would use this option to grant temporary entitlement access to a user.
- **Description** — Enter a brief description.

You may also have the option or be required to enter or select answers to questions about the request that request approvers or fulfillers or both require to complete their tasks. If user access or segregation of duties rules are implemented on the system, you may see the violations that would occur if the request were fulfilled. Although you may see the violations, however, you may or may not be able to submit the request.

Consult you access request administrator if you have any questions regarding these options.

Request Entitlement Access for Yourself

You can request access for yourself to all any of the entitlements the Access Request Manager administrator deems appropriate for you to choose from a list of entitlements similar users have.

To request access for yourself:

1. Click **Manage Access** on the **Home** dashboard.
2. Click **Add** for **My Access**.

   The Select Entitlements window appears.
3. Select the request source for which you want to request access, or, if multiple forms have been associated with the source, select one of the forms that appear when you click the request source.

   An access request form for the request source appears.
4. Choose the entitlements you want to request, and then click **Next**.
5. Answer any questions that may appear, specify a fulfillment or revocation date as required, configure request variables as required, and then click **Finish**. See "About Request Submission Procedure Options" on page 102 for more information.

   A confirmation window appears indicated that your request was submitted. You can verify that RSA IMG has generated the request by checking your **My Requests** dashboard component. It lists all pending change requests that you have initiated.

Request Entitlement Access for Another User

You can request access for users you are entitled to view. Consult your Access Request Manager administrator if you have questions about the user views available to you.

To request access for a user:

1. Click **Manage Access** on the **Home** dashboard.
2. Click **Add** for **Other's Access**.

   A user selection window appears. It lists the users for whom you are entitled to request access.
3. Select one or more users, and then click **Next**.

   An access request form for the request source appears.
4. Choose the entitlements you want to request, and then click **Next.**
5. Answer any questions that may appear, specify a fulfillment or revocation date as required, configure request variables as required, and then click **Finish**. See "About Request Submission Procedure Options" on page 102 for more information.

   A confirmation window appears indicated that your request was submitted. You can verify that RSA IMG has generated the request by checking your **My Requests** dashboard component. It lists all pending change requests that you have initiated.

Changing Access

You can change access for yourself and users for whom you are entitled to change access. Change access options enable you to do the following:

- Request changes in entitlement access for yourself or other users.
- Request entitlement removal for yourself or other users.

Request Changes in Entitlement Access for Yourself

When you change access for yourself, you can request entitlement access and removal of entitlement access.

To request changes in entitlement access for yourself:

1. Click **Manage Access** on your home page dashboard.
2. Click **Change** for **My Access**.

   A list of your entitlements appears.
3. Click **Remove** to specify the entitlements you want to relinquish, click the **Add Entitlements** button and select entitlements if you also want to request entitlements, and then click **Next.**
4. Answer any questions that may appear, specify a fulfillment or revocation date as required, configure request variables as required, and then click **Finish**. See "About Request Submission Procedure Options" on page 102 for more information.

A confirmation window appears indicated that your request was submitted. You can verify that RSA IMG has generated the request by checking your My Requests dashboard component. It lists all pending change requests that you have initiated.

Request Changes in Entitlement Access for Another User

When you change access for another user, you can request entitlement access and removal of entitlement access.

To request changes in entitlement access for another user:

1. Click **Manage Access** on your home page dashboard.
2. Click **Change** for **Other's Access**.

   A user selection window appears. It lists users for whom you are entitled to change access.
3. Select the user for whom you want to change access, and then click **Next**.

   A list of the user's entitlements appears.
4. Click **Remove** to specify the entitlements you want to remove, click the **Add Entitlements** button and select entitlements if you also want to request entitlements, and then click **Next.**
5. Answer any questions that may appear, specify a fulfillment or revocation date as required, configure request variables as required, and then click **Finish**. See "About Request Submission Procedure Options" on page 102 for more information.

   A confirmation window appears indicated that your request was submitted. You can verify that RSA IMG has generated the request by checking your My Requests dashboard component. It lists all pending change requests that you have initiated.

Requesting Changes in Access From the "Other Changes" Button

The **Other Changes** button appears in all change access forms and also under a user's details view **Access** tab if the **Allow access changes on a user's detail Access tab** setting is enabled as described in "Specifying Access Request Settings" on page 18. It enables you to do the following:

- Request access to a particular application.
- Compare entitlements that other users have. This option is available only if the **Users can compare access to other users** option is enabled as described in "Specifying Access Request Settings" on page 18.
- Request removal of entitlements that are in violation of user access or segregation of duties rules.
- Request removal of out-of-constraint roles.

Request Access to a Particular Application

You can request access to particular applications for yourself and other users.

To request access to an application:

1. In the user details view under the **Users** menu, click **Access**.

2. Click **Other Changes**, and select **Add entitlements for an application**.

   By default, a list of **Current Applications** from the drop-down list appears. It includes only those applications for which the user currently has entitlements. You can display a list of all applications for which you can request access by selecting the **All Applications** option. An Access Request Manager administer may have included additional custom applications view for you that you can select from.

3. Select the application for which you want to request entitlements, and then click **Select Entitlements**.

   A window enabling you to select entitlements for the application appears. You can choose **Suggested Entitlements** to display entitlements that similar users have, or you can choose **All Entitlements** to display all entitlements for the application.

4. Select the entitlements, and then click **OK**.

Change Access Based on a Comparison with Another User

You can determine which entitlements you or another user should and should not have based on a comparison with another user who has the entitlement set you or another user should have. Then you can request changes to your access to synchronize your or another user's entitlements with those of the comparison user.

You would do this when you want to ensure that you or another user have the same entitlements as someone else who has, for example, an identical job code or project responsibilities or department or group affiliation.

To change access based on comparison:

1. In the user details view under the **Users** menu, click **Access**.
2. Click **Other Changes**, and select **Compare with user**.
3. Choose a view of the users you are entitled to view from the drop-down list. For example, you may be able to view **Direct Subordinates** (if you are a supervisor) or any other custom user view configured by an Access Request Manager administrator for you.
4. Select a user for comparison, and then click **Compare Users**.

   A window appears with a list of entitlements for which you can request adds and removals. If the comparison reveals that you or another user have the same entitlement set as the comparison user, no entitlements are listed.

5. Click **Add** for entitlements you or another user should have or **Remove** for entitlements you or another user should not have, and then click **OK**.

   A list of entitlements to add or remove or both appear.

6. Click **Submit Request**.

   The Access Request window appears. It lists your request items. Configure any options available to you and proceed through the wizard to answer any questions presented to you. See "About Request Submission Procedure Options" on page 102 for more information.

7. Click **Finish**.

A confirmation window appears indicating the request has been created.

Request Removal of Violating Access

You can request removal of your or another user's entitlements that violate a user access or segregation of duties business rule.

To request removal of violating access:

1. In the user details view under the **Users** menu, click **Access**.
2. Click **Other Changes**, and select **Remove violating access**.

   A list of violating access entitlements appears.
3. Click **Remove** for each entitlement, or click **Remove All** to remove all entitlements.
4. Click **OK**.
5. Click **Submit Request**.

   The Access Request window appears. It lists your request items. Configure any options available to you and proceed through the wizard to answer any questions presented to you. See "About Request Submission Procedure Options" on page 102 for more information.
6. Click **Finish**.

   A confirmation window appears indicating the request has been created.

Request Removal of Out-of-Constraint Roles

An out-of-constraint role is a role in which you or another is a member but you should not be a member based on the membership rules configured for the role. For example, if a role's membership policy stipulates that only those who belong to the Accounting department should be a member of a role and you are not a member of the department and have the role, you can request removal from that role.

To request removal of membership in an out-of-constraint role:

1. In the user details view under the **Users** menu, click **Access**.
2. Click **Other Changes**, and select **Remove out-of-constraint roles**.

   A list of out-of-constraint roles appears.
3. Click **Remove** for each role.
4. Click **Submit Request**.

   The Access Request window appears. It lists your request items. Configure any options available to you and proceed through the wizard to answer any questions presented to you. See "About Request Submission Procedure Options" on page 102 for more information.
5. Click **Finish**.

   A confirmation window appears indicating the request has been created.

Requesting Creation of a New User

Important: *This section assumes all preparation tasks required to support new user requests have been completed in RSA IMG. If you are a system administrator, see* *Chapter 10, "Set Up the System for New User Registration Requests," on page 81* *for more information.*

You can request creation of a new user in an Active Directory (AD) data source using a form or a web services command:

- The "register user" form type prompts you to provide input that is required to fulfill the request to create the new user. Consult your system administrator for information on how to access the form. It may be available from a request button or as a menu option.
- The "createChangeRequest" web services command enables you to provide all of the inputs required to create the new user. See the instructions under the createChangeRequest command in the web services user interface. See for more information and consult your system administrator for information on using web services.

To request creation of a new user:

1. Invoke the **Register User** request form. The system administrator may or may not have created a request button for this request type. Consult your system administrator for more information on how to invoke the register user request form.
2. Enter information about the new user in the form:
   - **First Name** — The new user's first name.
   - **Last Name** — The new user's last name.

   In addition to this mandatory information, you might be required to enter an email address for the recipient (the new user in most cases) of the new user's AD directory account name and password. This email is generated once the user has been created in the AD directory and collected into RSA IMG.

   Note: *The first time the new user logs into the AD directory with this password, the user is prompted to change his or her password. Once the user is granted access to the AD domain, her or she is able to log in to RSA IMG using the directory as the authentication source.*

   Check with your system administrator about how to respond to other additional prompts for information in the form.

Checking the Status of the Register User Change Request

You can check the status of register user change request at any time during the approval and fulfillment phases. See "Accessing Requests" on page 235 in the *Administrators Guide* for information on viewing requests. Important information about the request is available from the Provisioning Changes table in the change request:

- The **Comments** icon under the Status column opens a window that provides information about whether AFX succeeded or failed to create the user account in the directory endpoint. In the case of a failure, the changes may need to be manually fulfilled or the request might have to be cancelled and then resubmitted when the problems that caused the failure are identified and corrected.

- The **Attributes** link under the Attributes column displays a table listing the attributes that will be created in the directory by the AFX "Create an Account on a AD server" command. All encrypted attributes (Password for example) are masked. Unencrypted attributes are displayed in plain text.
- The **State** column indicates whether the request has been fulfilled but is pending verification of the new user in collected data, or that the data has been collected, the new user has been verified, and the request has been completed. Check with your system administrator if data collections have occurred but the new user is not listed under the **Users** menu.

You can also use the "getChangeRequestStatus" web services command to get the overall status of the change request. This command, however, does not provide any information about the success or failure of automated fulfillment by AFX. You can, instead, use the "getRequestItems" web services command to get more granular information. Consult your system administrator about using web services.

Requesting an Account Password Reset for Yourself

You can request an account password reset for yourself. As with any request, RSA IMG generates a change request to effect the change in the data source where account passwords are stored. Once the request is approved and fulfilled, RSA IMG generates notification email for you that provides a link to your **My Passwords** table where you can view the password and confirm that it has been reset.

Note: *See "Requesting a User Password Reset After a Failed Login Attempt" on page 22 in the Administrators Guide for information on how to request an RSA IMG login password reset if you have forgotten your login password.*

To request an account password reset:

1. Click **Manage Access** on your home page dashboard.
2. Click **Reset** for **My Passwords**.

   A request form appears that lets you specify the account for which you want to change your password. It requires you to enter your account password before you can enter the new password. The password requirements (length, character restrictions, and so on) are specified by the password policy associated with the business source.

   Note: *Your account password reset request may generate additional password reset items in the request for accounts you have to other business sources. This password synchronization process may or may not be in effect for you. Consult your Access Request Manager administrator and see "Creating and Managing Account Password Synchronization Groups" on page 76 for more information.*
3. Select the account, enter your current account password (optional, the one you want to reset) and enter and confirm the new password, and then click **Finish**.

See "View Your New Password" on page 109 for information on how to retrieve your password.

View Your New Password

You can view your password once it has been reset in the appropriate data source. You can view your password once only. You can access the password from the link in the password reset notification email you receive or any time you are logged in to RSA IMG. You must view your password within the time period specified (default is 48 hours) after it has been reset. Otherwise, you must contact the account administrator to retrieve your password.

Note: *The number of hours you are allowed to view a password reset before it expires is configurable. Consult you system administrator if you require additional time to view your future password resets. If you are an administrator, see "Specifying System Settings" on page 36 in the Administrators Guide for more information on configuring a time limit.*

To view your password:

1. Click the **Users** menu and select **My Passwords** or click **View** for **My Passwords** on the **Manage Access** dashboard accessible from the Home page.

   The My Passwords table appears. It includes a record of your current password reset, previously viewed password resets, and expired passwords that where not viewed within the numbers of hours you were allowed to view them.

2. Click the **View Password** link in your current password reset entry.

   The View Password window appears. It displays your new password along with the account and the business source to which the account provides access. Once you close the window, the password reset entry in the My Passwords table changes to the "Previously Viewed" status.

View Your Password from an External URL

In the case where an account password has been requested for you or has been reset for a directory that serves as an RSA IMG authentication source, you can view the password from an external URL link in an email message sent to you by RSA IMG. (The email is sent to your supervisor as well by default.) The URL allows you to view the password once. After you view the password, you cannot view it a second time.

Email message example:

```
Hello Jane Doe,

A new password for Active Directory is available for one time view.

The password can be viewed at <URL link>.

Thank you
```

To view your password:

1. Go to the URL link in the email you received to access the View Password dialog box.
2. Enter your user name, and, if necessary, select the authorization source directory for which you want to view your account password.
3. Click **OK**.

   Your password appears.

View the Accounts for Which Your Passwords Are Expiring

You can view the accounts to which you have passwords that been previously reset that are expiring soon. This enables you to determine when you are going to have to request new passwords to those accounts.

To view your password:

1. Click the **Users** menu and select **My Passwords** or click **View** for **My Passwords** on the **Manage Access** dashboard accessible from the Home page.
2. Click the **Expiring Passwords** tab.

   A list of accounts, the business sources they provide access to, and the password expiration dates for the accounts appears. The system generates email notifying you about your soon-to-expire passwords and expired passwords.

Requesting an Account Password Reset for Another User

You can request an account password reset for another user if you have the correct privileges:

- You are a system administrator.
- You are a business or technical owner of the business source to which the account provides access.
- You have been granted the "Reset Password" entitlement. See Chapter 6, "Managing RSA IMG Application Privileges," on page 103 for more information.

As with any request, RSA IMG generates a change request to effect the change in the data source where account passwords are stored. Once the request is approved and fulfilled, RSA IMG generates notification email for the user that provides a link to his or her **My Passwords** table where he or she can view the password and confirm that it has been reset.

To request an account password reset for another user:

1. Click **Manage Access** on your home page dashboard.
2. Click **Reset** for **Others' Passwords**.
3. Select the user for whom you want to change an account password, and then click **Next**.

   A request form appears that lets you specify the account for which you want to change the password.

   Note: *Your account password reset request may generate additional password reset items in the request for accounts the user has to other business sources. This password synchronization process may or may not be in effect for the user. Consult your Access Request Manager administrator and see "Creating and Managing Account Password Synchronization Groups" on page 76 for more information.*
4. Select the account for which you want to reset the user's password. A password is randomly generated. Click **Next**.
5. Click **Finish**.

   Once the user's account password has been reset, he or she can view the new password under his or her **Users > My Passwords**.

Requesting Termination of Users

You can request immediate or scheduled termination for one or more users. This enables you to perform a termination action and disable terminated user accounts on an on-demand basis instead having to wait for an provisioning - termination rule to trigger and initiate account removal actions. See Chapter 4, "Rules," on page 129 for information on creating a provisioning - termination rule. Once a termination is fulfilled, a terminated user's "Is Terminated" attribute is updated to "Yes."

To request termination to one or more users:

1. From the **Create Request** button, click **Terminate Users**.
2. Select the users for whom you want to request termination.

   The Default Termination Form or any other customized version of the form appears.
3. Configure the form as follows:
   - **Termination Date** — Select the date of the termination, the current date or a future date.
   - **Disable Accounts in Request** — Select this option if you want the accounts the terminated users have to be disabled.
   - **Comments** — (Recommended) Enter comments that provide business justification for the termination request
   - **Attachments** — (Recommended) Attach any documentation that supports the termination request.
4. Click **Next**.
5. Review and make any adjustments to your request, and then click **Finish**.

   The request is submitted for approval and fulfillment.

To request termination for a single user from the user's details view:

1. From the user's **Access** tab, select **Terminate** from the **Other Changes** button.
2. Proceed through the request process as described above.

Requesting Leave of Absence for Users

To ensure that access to your organizations's resources is temporarily suspended for users who take a leave of absence (extended vacation for example) for the duration of the leave, you can generate of a leave of absence request. The request requires you to specify the leave start and return dates. It also specifies the suspension actions that must be competed: whether the passwords for any of the shared accounts the user has should be reset or whether user accounts should be disabled or both.

To request leave of absence:

1. From the **Create Request** button, click **Leave of Absence**.
2. Select the user for whom you want to request a leave of absence.

   The Default Leave of Absence Form or any other customized version of the form appears.

3. Configure the form as follows:
   - **Leave Start Date** — Select the date the user begins the leave.
   - **Reinstatement Date** — Select the date the user returns from the leave.
   - **Reset Shared Accounts** — Reset the password for the accounts the user shares with others.
   - **Disable Accounts** — Select this option if you want the accounts the ‘11user has to be disabled.
   - **Comments** — (Recommended) Enter comments that provide business justification for the leave of absence request
   - **Attachments** — (Recommended) Attach any documentation that supports the leave or absence request.
4. Click **Next**.
5. Review and make any adjustments to your request, and then click **Finish**.

   The request is submitted for approval and fulfillment.

To request termination for a user from a user’s details view:

1. From the user’s **Access** tab, select **Take a Leave of Absence** from the **Other Changes** button.
2. Proceed through the request process as described above.

Requesting Account Management Actions

You can request the following account management actions for user accounts for business sources that support the following actions:

- Enable a disabled account.
- Disable an enabled account.
- Lock an unlocked account.
- Unlock a locked account.

See Chapter 12, “Creating and Managing Applications,” on page 165 and Chapter 13, “Creating and Managing Directories,” on page 181 in the *Administrators Guide* for instructions on how to designate those application and directory business sources, respectively, as supporting the account management actions. This lets you explicitly initiate account management actions on an on-demand basis without having to rely entirely on account actions being initiated via advanced provisioning rules.

To request an account management action:

1. From the **Create Request** button, click **Manage Accounts**.
2. Select one or more users for whom you want to take an action.

   The Default Account Management Form or any other customized version of the form appears with a list of accounts for the selected users.

3. Click the button for the action you want to perform for each account. For example, click **Lock** for an account to include the lock action to the change request.
4. Click **Next**.
5. Configure the following optional settings:
   - **Description/Notes** — Add any information that will assist change request participants make informed decisions, why the actions should be fulfilled for example.
   - **Fulfillment Date** — Specify a date on which you want the action fulfilled in the data source. This setting allows you to delay the action.
   - **Revocation Date** — Specify a date upon which RSA IMG will automatically generate a change request for the action. This option allows you to delay the change request.
6. Review your request, and then click **Finish**.

   The request is submitted for approval and fulfillment.

To request an account management action from a user's details view:

1. From the user's **Access** tab, select **Manage User's Accounts** from the **Other Changes** button.
2. Proceed through the request process as described above.

Requesting Fulfillment of Business-Source-Specific Commands

In some cases, you may want to fulfill a command supported by a business source that you cannot request directly in RSA IMG, create a group for example. This section uses a simple "create a group" example to illustrate how to set up the request form for this type of request and generate the request.

Note: *See "Configure Provisioning Command Node Properties" on page 268 in the Administrators Guide for information on how to run provisioning commands via an AFX fulfillment workflow. This is an alternative method to the one described in this section that does not involve an explicit request to complete the commands on an business source.*

To set up requirements for this request type:

1. Create an AFX connector ("Create_Group_Connector" for example) to fulfill the create group command on a business source. For example, the database connector type supports the "Create a Group" command. See Chapter 4, "Creating and Managing AFX Connectors," on page 31 in the *Access Fulfillment Express Guide* for more information.
2. Bind the Create_Group_Connector to the business source (application or directory) where you want the command fulfilled. See Chapter 5, "Managing Automatic Request Fulfillment for Business Source Endpoints," on page 43 in the *Access Fulfillment Express Guide* for more information. Ensure also that an AFX fulfillment workflow (Default AFX Fulfillment for example) is associated with the business source.

3. Create a global form with the Provisioning Command (Non-Visual) control type. See Chapter 4, "Creating and Managing Access Request Forms," on page 27 for more information.

   Configure as follows:

   - Name: "Create_Group_Form."
   - Add variables to the form:
     - Variable_1 — Static Text control type: "This form lets you create a group."
     - Variable_2 — Text control type: "Group Name"
     - Variable_3 — Provisioning Command (Non-Visual) control type.

4. Configure the Provisioning Command (Non-Visual) control type:

   - Select the business source to which you bound the Create_Group_Connector.
   - Select the Create a Group command that is supported by the business source.
   - Select the ${avform.groupname} variable under **Parameters**.

   You can now choose to create a request button for the form and make it available to users along with other request buttons, or you can simply run the form using the form's **Run Form** button.

5. Generate the change request.

6. Provide the name of the group you want created in the **Group Name** field, and then click **Next**.

7. Review the request details to confirm that you have correctly requested that the Create a Group command be completed on the business source you specified, and then click **Finish**.

   The request is processed. The group you created is verified by the system upon the next group data collection.

Index

A

C

D

E

F

L

M

N

O

P

R

S

T

U

V

W