Adaptive Risk Manager Offline
Administrator's Guide
10g Release (10.1.4.3.0)

December 2007

ORACLE

Adaptive Risk Manager Offline Administrator's Guide, 10g (10.1.4.3.0)

Contents

Preface

Adaptive Risk Manager Offline is an offline fraud analysis tool for evaluating existing transaction data. It can be used in two ways:

- As a stand alone security tool to analyze, detect, and alert high risk transactions.
- In conjunction with Adaptive Risk Manager Online as a supplemental offline analysis tool and as a way to pre-visualize rules against real customer data without impacting customers in real-time environment.

The Adaptive Risk Manager Offline Administrator’s Guide provides information on creating database configurations and using Adaptive Risk Manager Offline to evaluate existing transaction data.

Related Documentation

The Oracle Adaptive Access Manager Offline 10g documentation includes:

- The Oracle® Adaptive Access Manager Offline Dashboard and Reporting Guide
- The Oracle® Adaptive Access Manager Offline Customer Care Guide
- The Oracle® Adaptive Access Manager Offline Managing Data Guide

Introduction

Adaptive Risk Manager Offline is a configuration and investigation tool for analysis and development of risk mitigation strategies.

It provides the ability to:

- Conduct offline analysis using historical data to investigate fraudulent activity.
- Load historical data from a real-time Adaptive Risk Manager database or from an institution's logging/auditing data sources.
- Test the effectiveness of models and rules without impacting the production system and production performance

This guide is intended for use by rules administrators who configure Oracle Adaptive Access Manager using Adaptive Risk Manager Online and by investigators and analysts.

When using Adaptive Risk Manager Offline to conduct research and analysis, you might need to import the models and groups along with the data just as they appear in the online version, or you might need to create custom models that are different from the online models.

In either case, this guide provides step-by-step instructions for creating and managing groups, creating models that contain rules, customizing and managing rules, and managing the KBA functionality.

Groups

Grouping allows you to view and administer a collection of like items as a single group. To simplify administration, you should assign each group a unique name.

You can create the following types of groups:

- User ID – A User ID group is a collection of User IDs to which you can assign a set of authentication and authorization rules.
- Login ID – A Login ID group is a collection of Login IDs used for Phish Baiting exercises.
- Location – There are a number of group types for location information. Each type of location has its own group type, these include cities, states, countries, IPs, and IP ranges.
- Device – A device group is a group of device IDs.
- Action – An actions group is a set of responses that are triggered by a rule.
- Alerts – An alert group contains graded messages that can be triggered by a rule.
- ASN (Autonomous System Number) - A unique identifier of an autonomous system on the Internet.
- ISP (Internet Service Provider) – An internet connection service business utilized by users hitting the system.
- Top Level Domains (TLD) - Identifies the most general part of the domain name in an Internet address.
- Secondary Level Domains (SLD) - Identifies part of the domain name in an Internet address.
- IP Carriers - Custom IP location data from IP vendor database
- Routing Type - Custom IP location data from IP vendor database
- Connection Type - Custom IP location data from IP vendor database

- Connection Speed - Custom IP location data from IP vendor database
- Generic Strings - List of strings used in rule conditions
- Generic Integers - List of integers used in rule conditions
- Generic Longs - List of longs used in rule conditions

Models

A model contains configured rule instances (or copies) that, once linked to a group, are used to evaluate activity of group members. The rules are added to the model, configured, and linked to groups by the administrator. New rule instances can be added to an existing model at any time. Model policy types include:

- Security
- Business
- Workflow
- 3rd Party

Rules

A rule identifies and reacts to certain information. Rules can be used for business or security purposes. Rules can be applied to specific groups of users or all users hitting the system.

Scores & Weights

Score refers to the numeric scoring used to evaluate the risk level associated with a specific situation. Weight refers to the multiplier value used to influence the total score at various evaluation levels.

Policies

A policy is a collection of models of the same type. The four policy types are:

- Security
- Business
- Workflow
- 3rd party

Policy Sets

The policy set is the collection of all the currently configured policies used to evaluate traffic in order to identify possible risk.

Organizing Users, Locations, and Devices into Groups

Adaptive Risk Manager Offline allows you to do everything that you do in Adaptive Risk Manager Online. It enables you to create groups for more efficient administration.

This section describes how to add items to groups individually. Auto-population and bulk uploads directly in the database are also available as part of the custom installation and integration process.

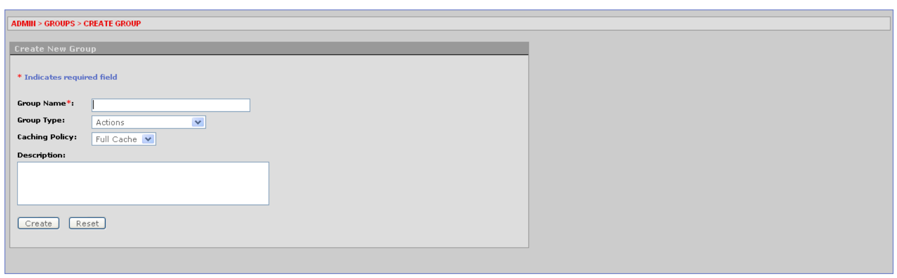
This section describes how to create and edit user ID, location, and device groups. This section includes:

- To create a new group of users
- To create a group of cities
- To create a group of states
- To create a group of countries
- To create a group of IPs
- To create a group of IP ranges
- To create a group of devices

To create a new group of user IDs

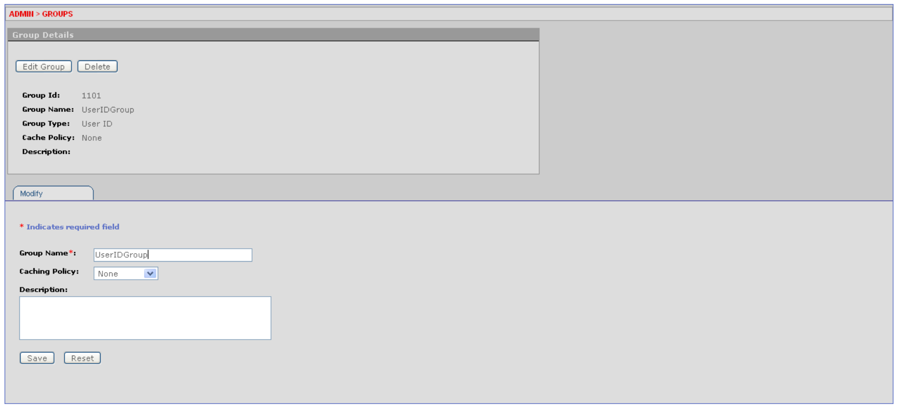
1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Group page appears.



2. **In the Group Name box, type a unique name for the group.**
3. **Click in the Group Type box and select User ID.**
4. **User groups do not support caching policy so it will be set to None.**
5. **Type any description and notes you want.**
6. **Click Create.**

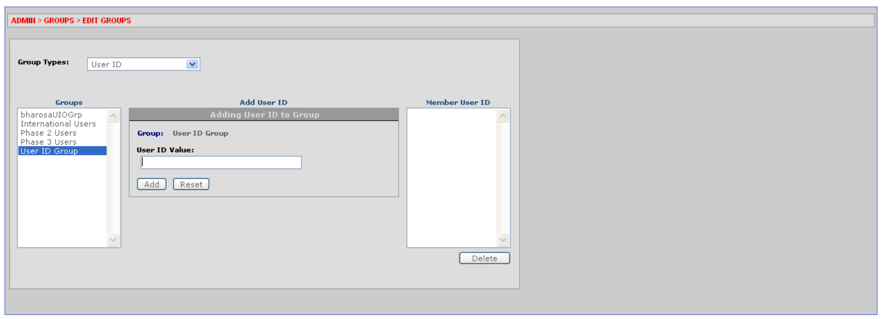
   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**

8. **Click Edit Group.**

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.



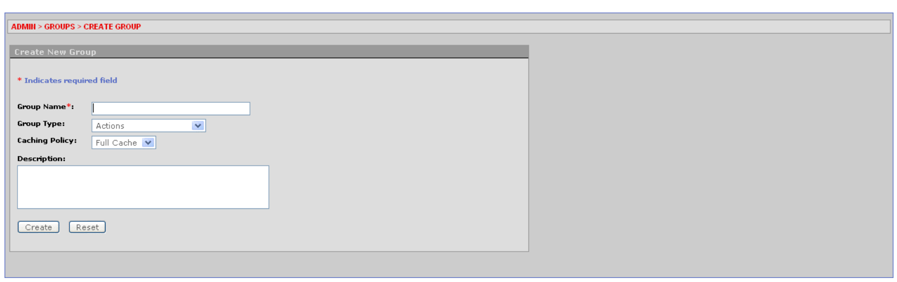
9. **In the User Id box, type the user Id of a user member you want to add to the group, and then click Add.**

   The User ID appears in the list of Member Users.

To create a group of cities

1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Groups page appears.



2. **In the Group Name box, type a unique name for the group.**

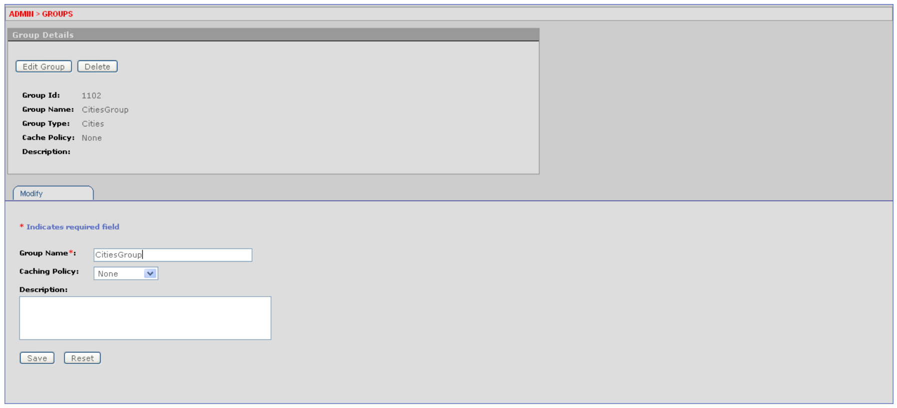
3. **Click in the Group Type box and choose Cities.**

4. **Click in the Caching Policy box and select the caching policy you want.**

5. **Type any description and notes you want.**

6. **Click Create.**

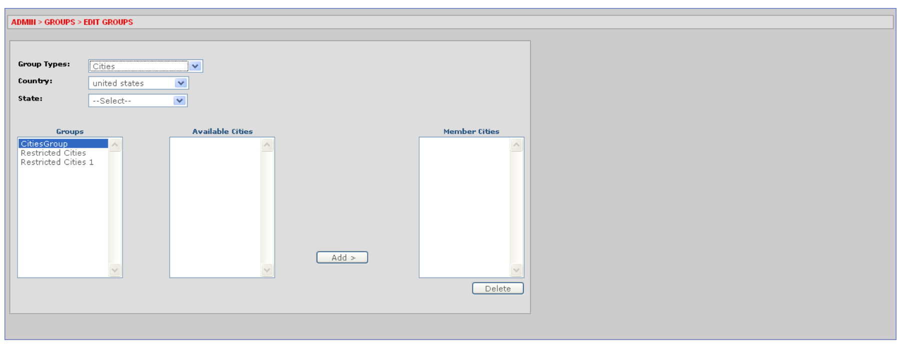
   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**

8. **Click Edit Group.**

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.



9. **Click in the Country box and choose the country you want.**

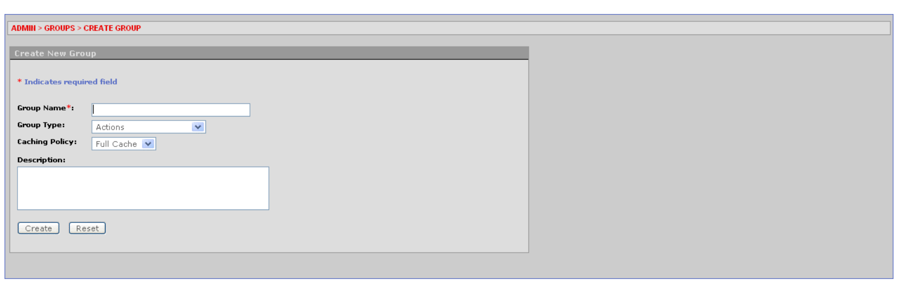
10. **Click in the State box and choose the state you want.**

11. **In the list of Available Cities, click the city you want to add, and then click Add.**

To create a group of states

1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Group page appears.

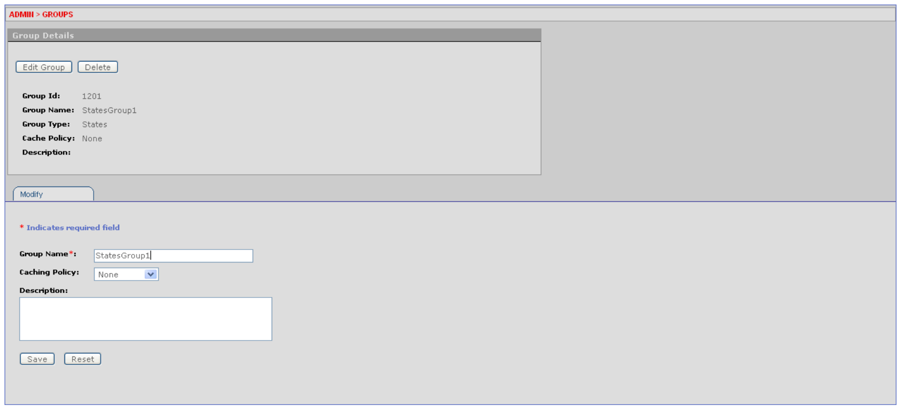


2. **In the Group Name box, type a unique name for the group.**

3. **Click in the Group Type box and choose States.**
4. **Click in the Caching Policy box and select the caching policy you want.**

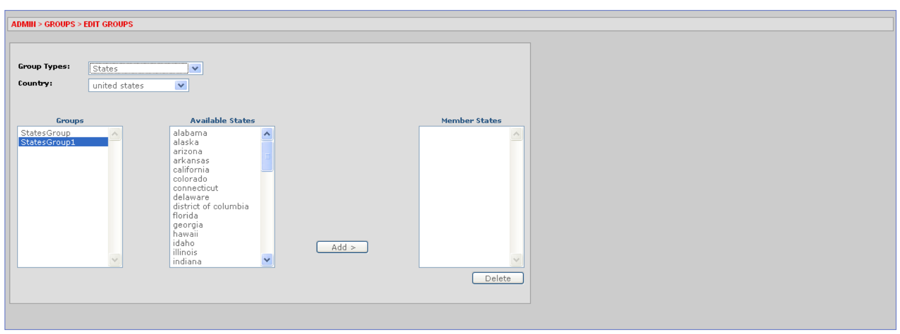
   Generally the full cache setting gives the best performance.
5. **Type any description and notes you want.**
6. **Click Create.**

   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**
8. **Click Edit Group.**

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.

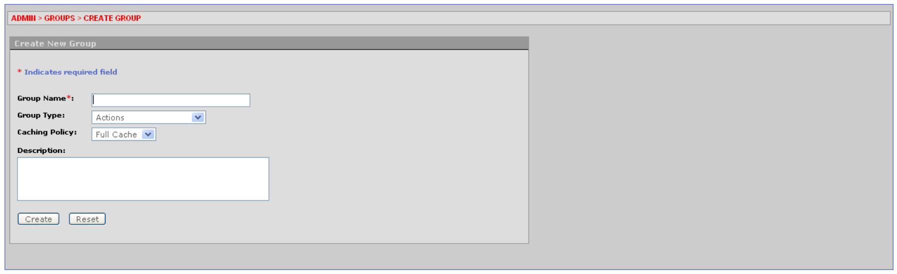


9. **Click in the Country box and choose the country you want.**
10. **In the list of Available States, click the state you want to add, and then click Add.**

To create a group of countries

1. **On the Admin menu point to Groups, and then click Create Group.**

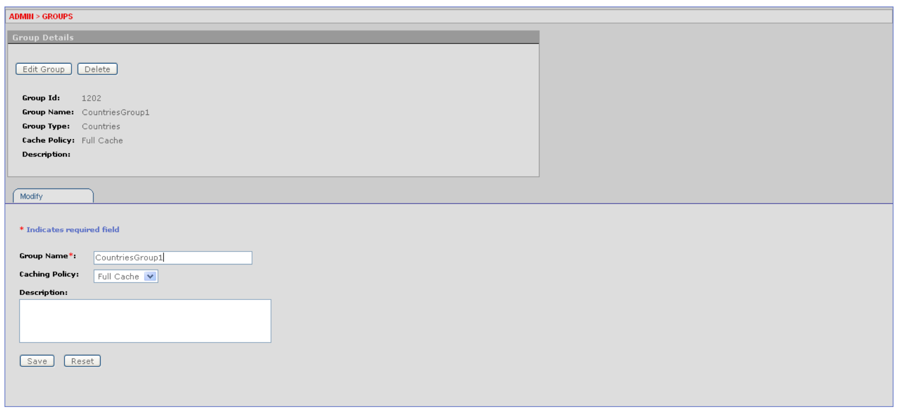
   The Create Group page appears.



2. **In the Group Name box, type a unique name for the group.**
3. **Click in the Group Type box and choose Countries.**
4. **Click in the Caching Policy box and select the caching policy you want.**

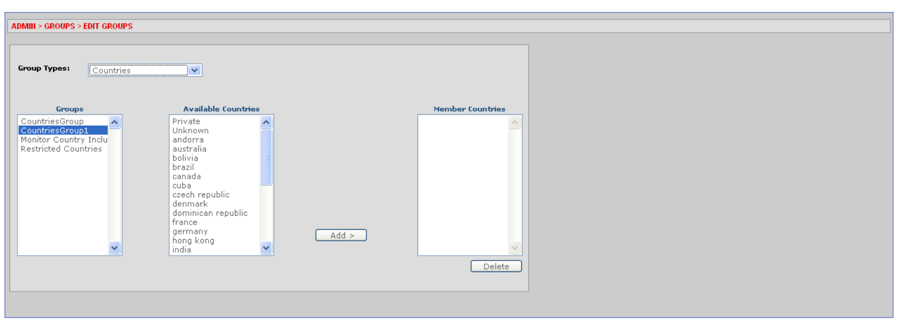
   Generally the full cache setting gives the best performance.
5. **Type any description and notes you want.**
6. **Click Create.**

   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**
8. **Click Edit Group.**

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.

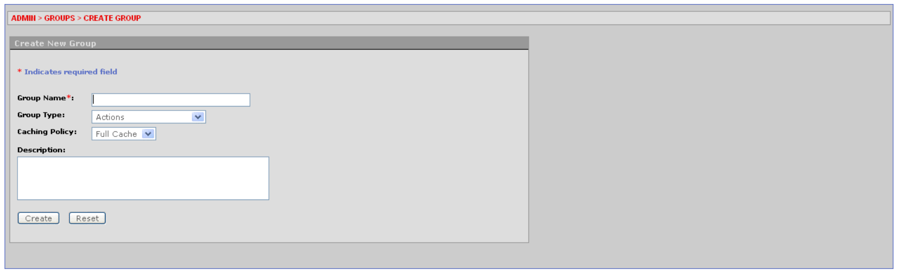


9. **In the list of Available Countries, click the country you want to add, and then click Add.**

To create a group of IPs

1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Group page appears.

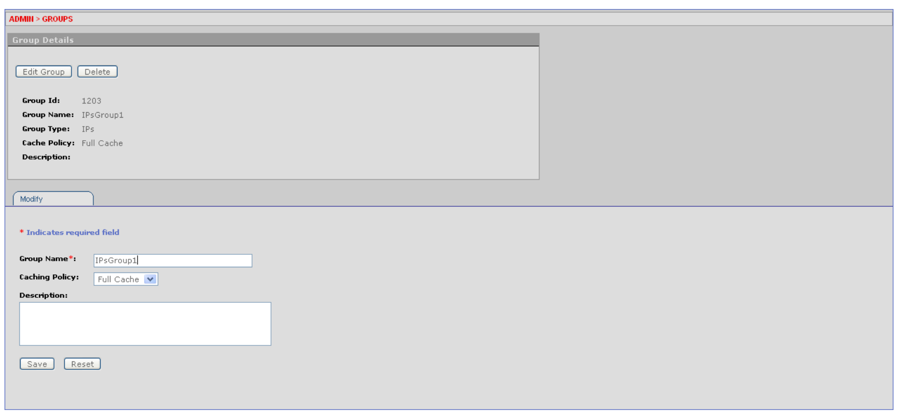


2. **In the Group Name box, type a unique name for the group.**
3. **Click in the Group Type box and choose IPs.**
4. **Click in the Caching Policy box and select the caching policy you want.**

   Generally the full cache setting gives the best performance.

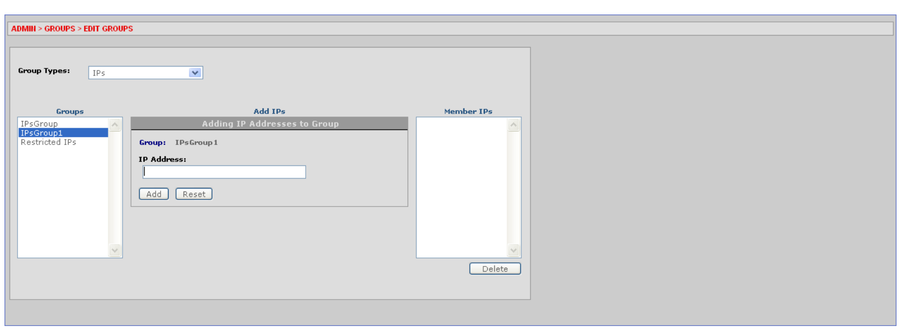
5. **Type any description and notes you want.**
6. **Click Create.**

   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**
8. **Click Edit Group.**

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.

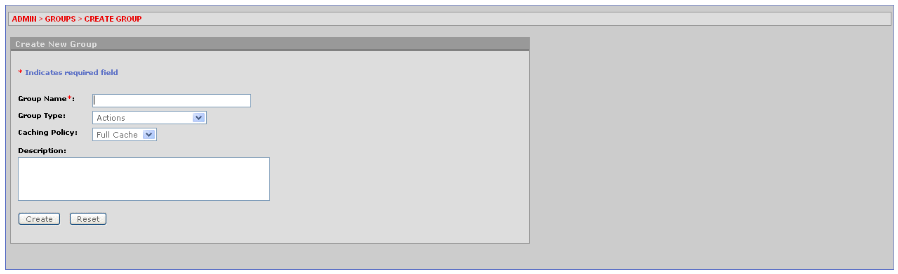


9. **Type the IP address you want to include in the group, and then click Add.**

To create a group of IP ranges

1. **On the Admin menu point to Groups, and then click Create Group.**

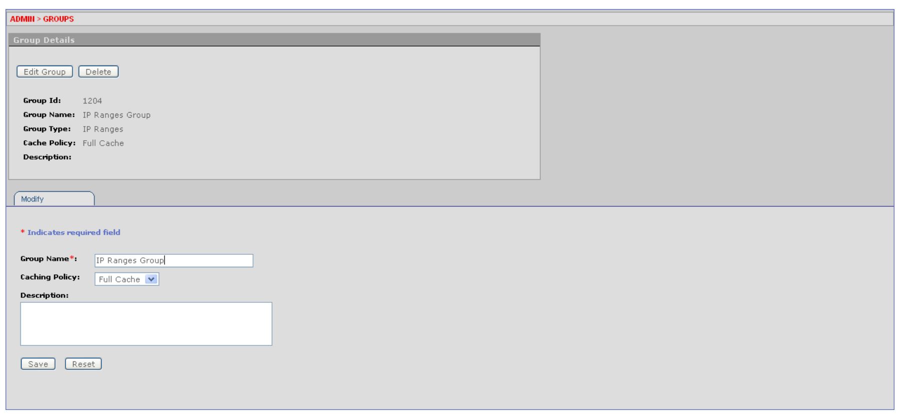
   The Create Group page appears.



2. **In the Group Name box, type a unique name for the group.**
3. **Click in the Group Type box and choose IP Ranges.**
4. **Click in the Caching Policy box and select the caching policy you want.**

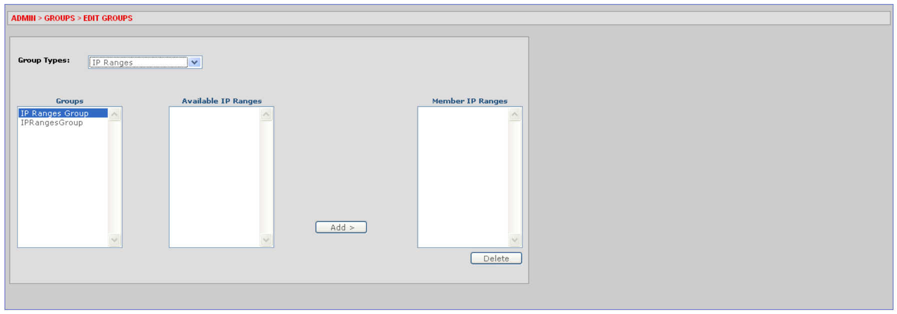
   Generally the full cache setting gives the best performance.
5. **Type any description and notes you want.**
6. **Click Create.**

   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**
8. **Click Edit Group.**

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.



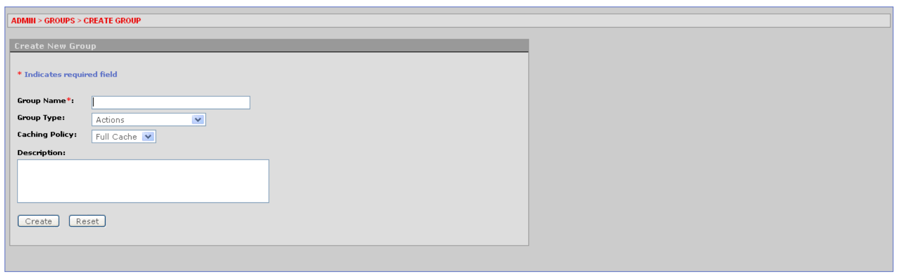
9. **Select from the list of Available IP Ranges, click the IP range you want to add to the group and click Add.**

   If none exist you can create new IP ranges from the Admin menu.

To create a group of devices

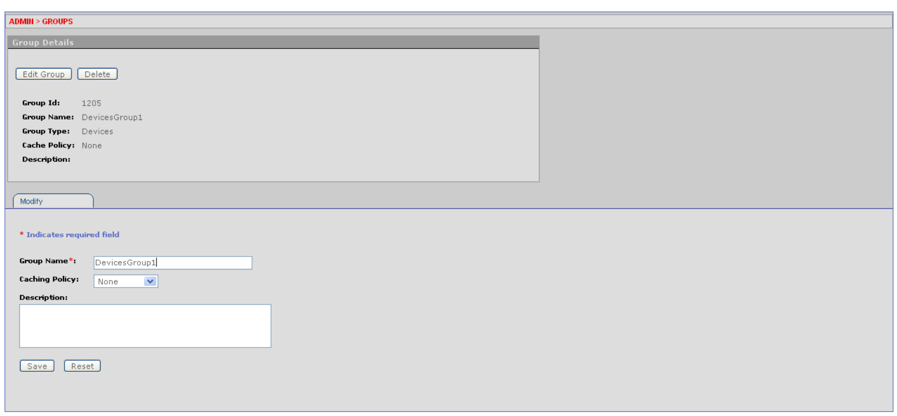
1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Group page appears.



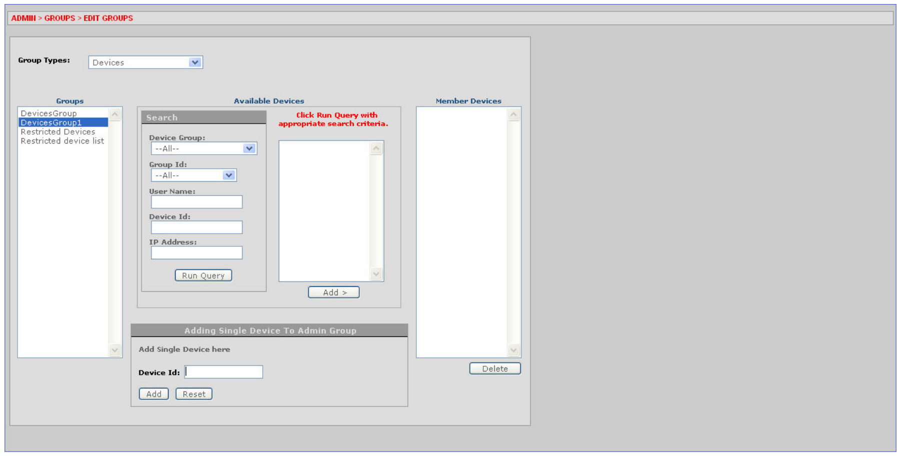
2. **In the Group Name box, type a unique name for the group.**
3. **Click in the Group Type box and choose Devices.**
4. **Click in the Caching Policy box and select the caching policy you want.**
5. **Type any description and notes you want.**
6. **Click Create.**

   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**
8. **Click Edit Group.**

The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.



9. **To search for devices, enter search criteria to limit returns and click Submit Query.**

10. **Select any number of devices from the list of available devices and click Add.**

11. **To add a specific device to the group without running a query, click in the Device ID box at the bottom of the page, type the device ID and click Add.**

Creating a Group of Alerts or Actions

Action groups and alert groups are used as results within rules so that when a rule is triggered all of the actions or alerts within the groups are activated.

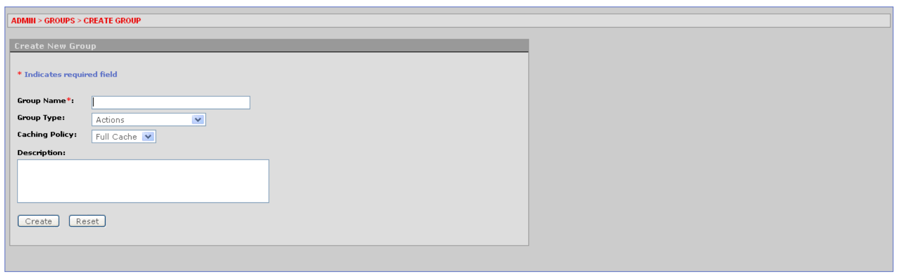
This section describes how to place a selection of actions into a group and how to configure/add alerts to a group. This section includes:

- To create an action group
- To create an alert group

To create an action group

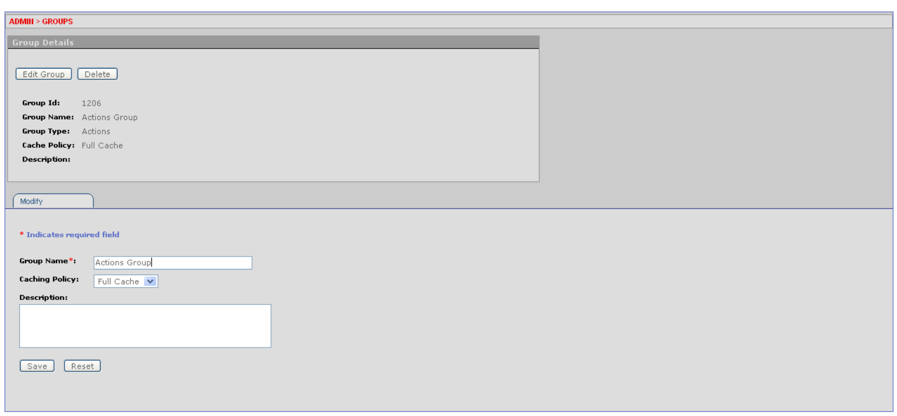
1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Group page appears.



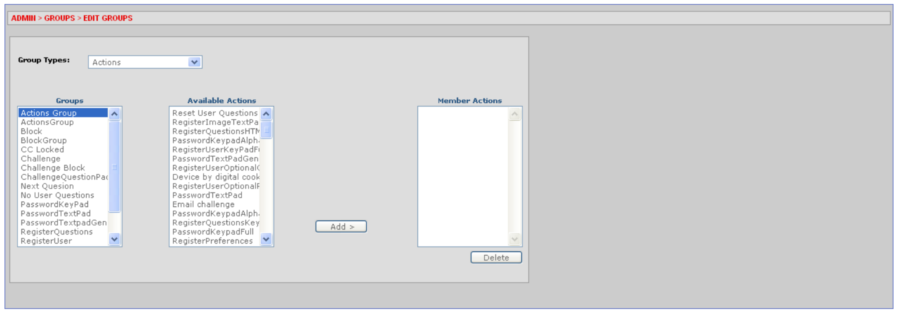
2. **In the Group Name box, type a unique name for the group.**
3. **Click in the Group Type box and choose Actions.**
4. **Action groups are always cached so Caching Policy should be set to Full Cache.**
5. **Type any description and notes you want.**
6. **Click Create.**

   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**
8. **Click Edit Group.**

The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.

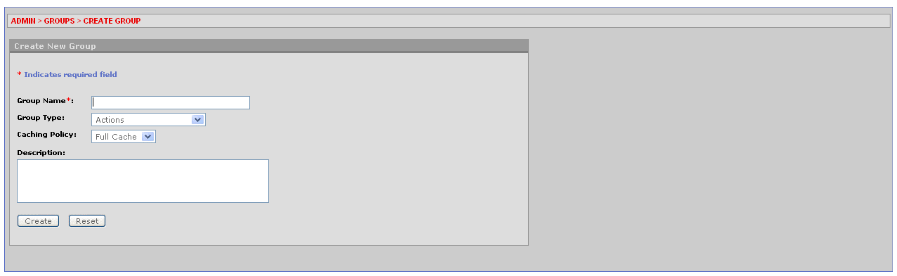


9. **In the list of Available Actions, click the action you want to add to the group, and then click Add.**

To create an alert group

1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Group page appears.



2. **In the Group Name box, type a unique name for the group.**

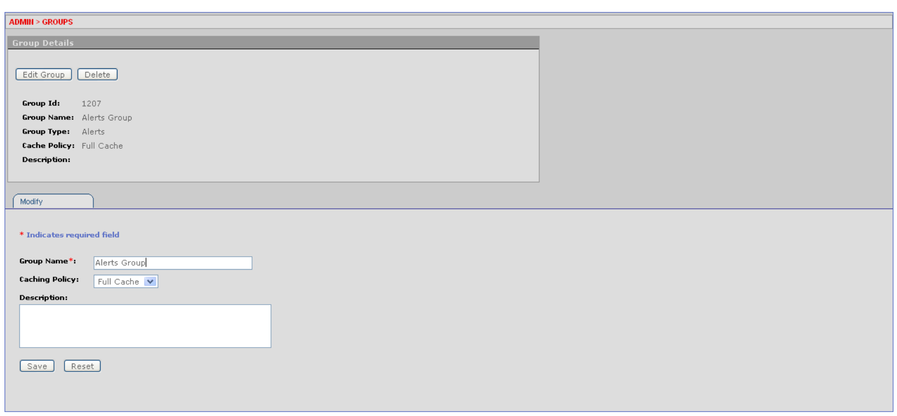
3. **Click in the Group Type box and select Alerts.**

4. **Alert groups are always cached so Caching Policy should be set to Full Cache.**

5. **Type any description and notes you want.**

6. **Click Create.**

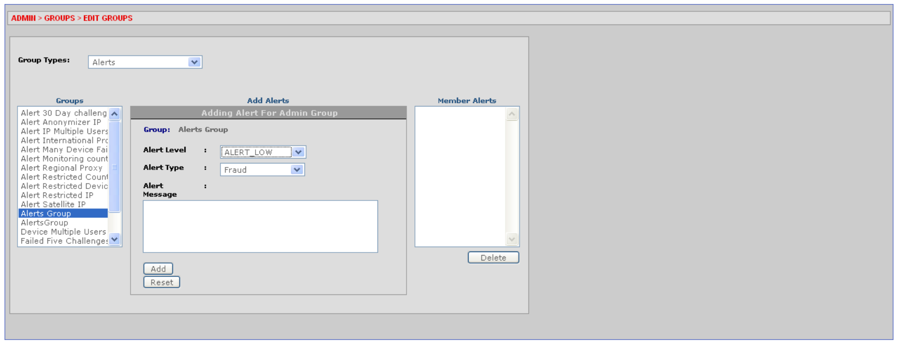
   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**

8. **Click Edit Group.**

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.



9. **Click in the Alert Level box and select the alert level you want.**
10. **Click in the Alert Type box and select the alert type you want.**
11. **Type an alert message. In most cases this message should correspond to the rule that will be configured to activate it.**
12. **Click Add.**

Creating Groups of Networks, Service Providers, and Systems

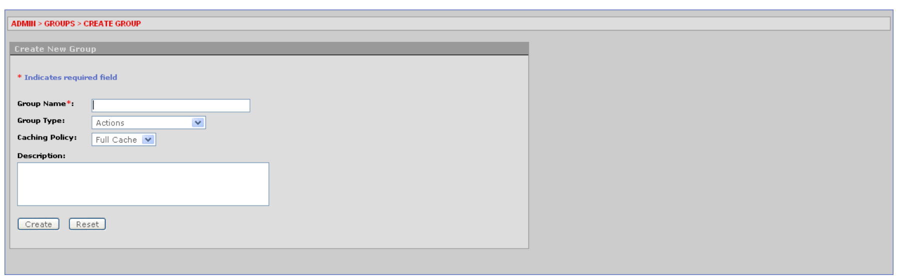
In addition to user, location, device, alert, and action groups, Adaptive Risk Manager Offline allows you to create these group types:

- ISP
- ASN
- Top Level Domains
- Second Level Domains
- Ip Carriers
- Routing Type
- Connection Type
- Connection Speed
- Generic Strings
- Generic Integers
- Generic Longs

To create a network, service provider, or system group

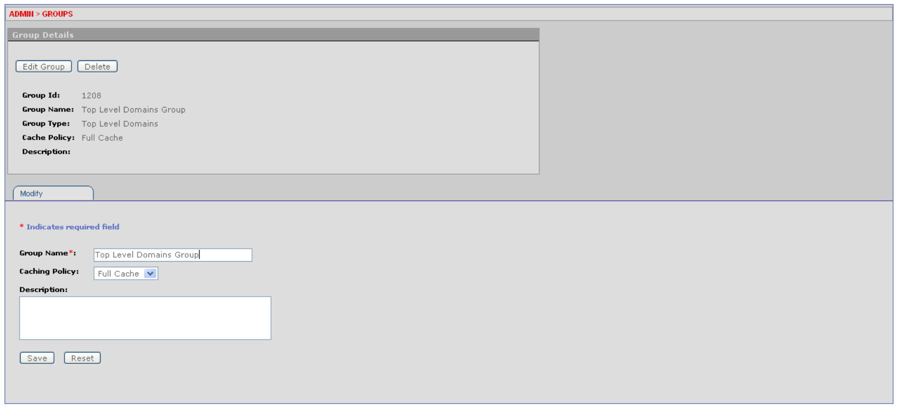
1. **On the Admin menu point to Groups, and then click Create Group.**

   The Create Group page appears.

2. **In the Group Name box, type a unique name for the group.**
3. **Click in the Group Type box and select the type you want.**
4. **Click in the Caching Policy box and select the caching policy you want.**
5. **Type any description and notes you want.**
6. **Click Create.**

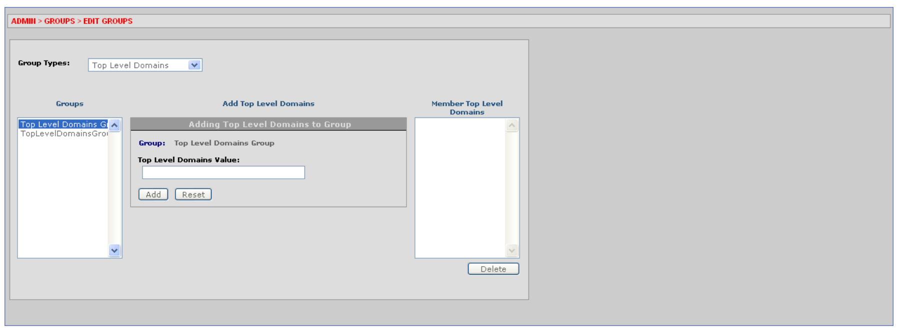
   The Group Details page appears.



7. **To change the group's name, type, or notes, see Viewing Details about a Group.**

8. **Click Edit Group.**

   The Edit Groups page appears. The group you are editing is pre-selected.



9. **In the String Value field, enter the value you want.**

10. **Click Add.**

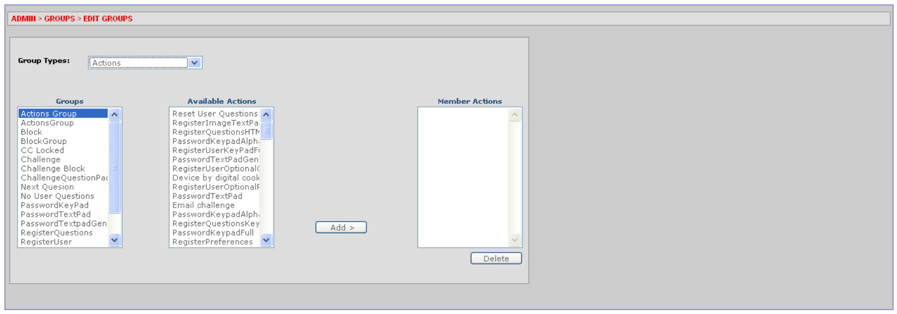
Editing a Group

You can edit a group whenever you want.

To edit a group

1. **On the Admin menu point to Groups, and then click Edit Groups.**

   The Edit Groups page appears.

2. **To filter the list of groups, click in the Group Type box and select the type you want.**

3. **In the list of Groups, select the group you want to edit.**

   The Edit Group page appears and displays the options appropriate for the type of group you selected.

4. **Add or delete members of the group as necessary.**

   For additional information, see Organizing Users, Locations, and Devices into Groups~~Organizing Users, Locations, and Devices into Groups~~ and Creating a Group of Alerts or Actions.

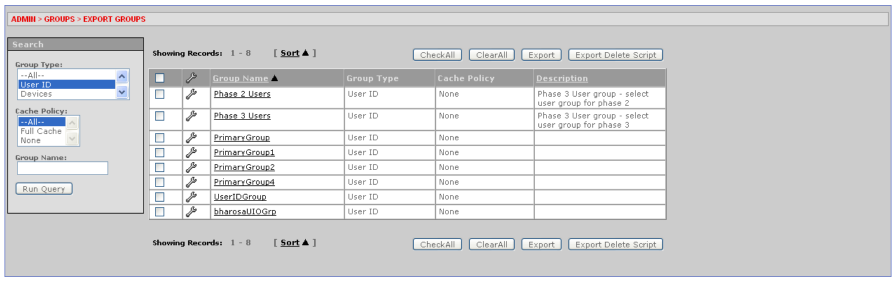
Exporting and Importing a Group

You can use the Export and Import Groups commands to export and import a group as an XML file.

To export a group

1. **On the Admin menu, point to Groups and click then click Export Groups.**

   The Export Groups page appears.



2. **Enter search criteria and click Run Query to locate the group.**
3. **Click the checkbox next to each group you want to export.**
4. **Click Export in the lower right corner of the page.**
5. **Click OK to the confirmation.**

   The Open dialog box appears.

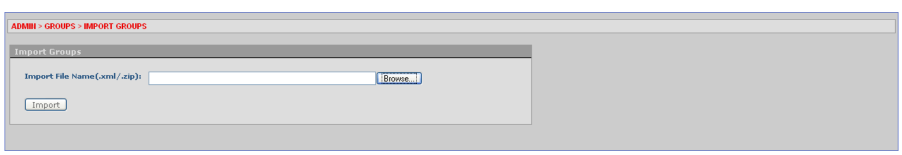
6. **Click Save To Disk and then click OK.**

   The file is exported.

To import and group

1. **On the Admin menu, point to Groups and click then click Import Groups.**

   The Import Groups page appears.



2. **Click Browse and locate the group file you want to import.**
3. **Click Import.**

   The group is imported.

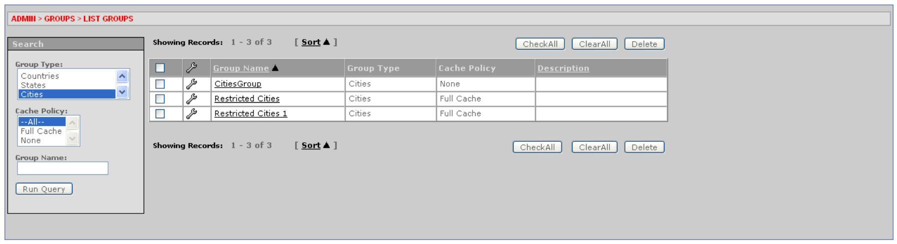
Viewing a List of Groups

On the List Groups page, you can view a list of all groups, a list of groups of a certain type, or you can view just one group. The List Groups page provides access to the Group Details page and the Edit Group page for any group.

To view a list of all groups

1. **On the Admin menu, point to Groups, and then click List Groups.**

   The List Groups page appears.

2. **To display only the type of group you want to edit, select the type you want from the Group Type list and click Submit Query.**
3. **To find a specific group, in the Group Name box enter the name of the group and click Submit Query.**
4. **To edit a group in the list, click the wrench icon to the left of the group you want to edit.**
5. **To view the Details for a group, click the Group Name.**

   See Viewing Details about a Group.

6. **To delete a group, select the checkbox to the left of the group name and then click Delete.**

   If the group is currently linked to a rule you will not be allowed to delete it.

Viewing Details about a Group

The Group Details page allows you to view or change details about a group.

To modify details about a group

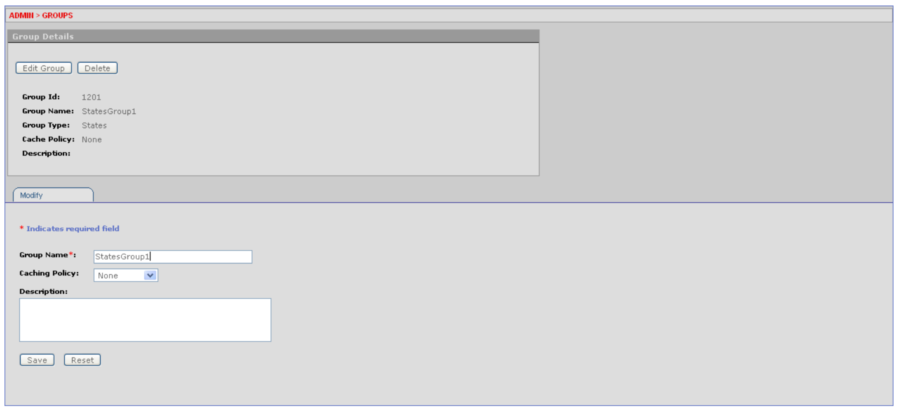
1. **On the Admin menu point to Groups, and then click List Groups.**

   The List Groups page appears.

2. **Select the search criteria you want and click Submit Query.**

3. **Click a group name to view the details page for that group.**

   The Group Details page appears.



4. **To change the group name, click in the Group Name box and type a new name and then click Save.**

Creating Models

A model is a collection of configured rule instances linked to User ID groups whose members are evaluated. Adaptive Risk Manager Offline enables you to create models that can be applied to more than one User ID group.

Oracle Adaptive Access Manager is shipped with groups, models and rules pre-configured. These models are set up using best practices for the client's specific industry and needs.

Model run time refers to the point during the session the rules in a model should be evaluated. By default there are eleven model run times in Adaptive Risk Manager Offline:

- Device Identification
- Pre-Authentication
- Post-Authentication
- In-Session
- AuthentiPad
- Preferences
- Challenge Question
- CC Challenge
- Forgot Password
- Invalid Login
- Wrong Password

Notes:

- In-Session models often require custom integration and therefore configuration is not covered as part of this Guide.
- In-Session models may not be supported in some UIO version 1.0 installations.

There are four *model policy types*. The policy types are Security, Business, Workflow, and 3rd Party.

To create a new model

1. **On the Admin menu point to Models, and then click Create Models.**

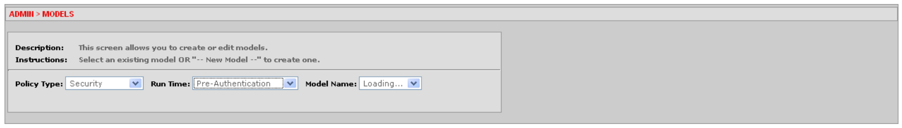
   The Policy Type menu appears.

2. **In the Policy Type list, click the type of model you want.**

   The Run Time menu appears.

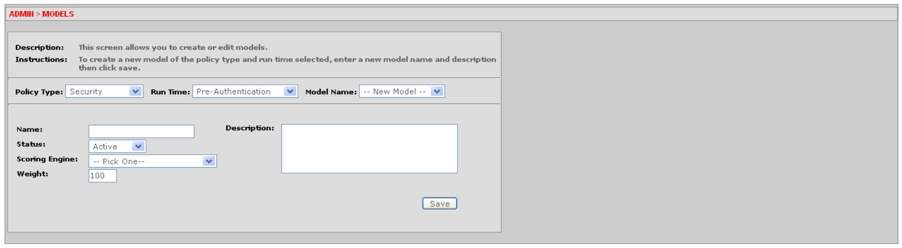
3. **In the Run Time list, click the run time you want.**

The Model Name menu appears.



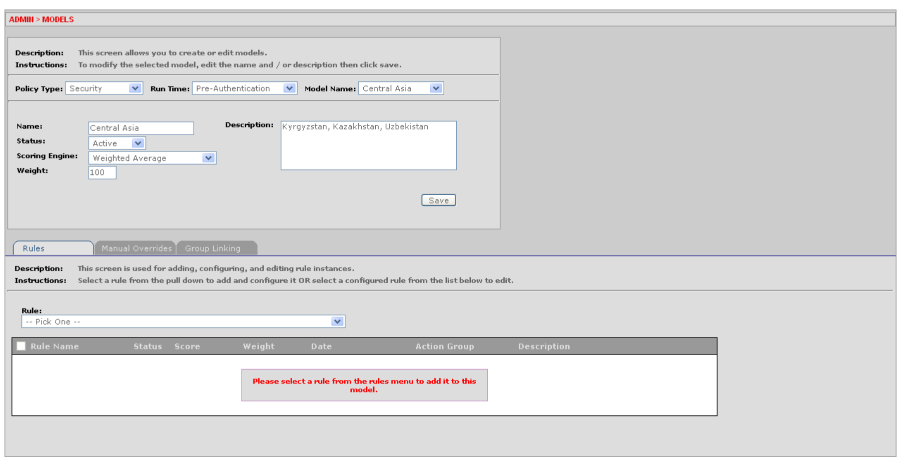
4. **In the Model Name list, click Create New Model.**

   The Create New Model page appears.



5. **In the Model Name box, enter a name for the model.**
6. **Click in the Status box and select the status you want.**
7. **Click in the Scoring Engine box and select the scoring you want.**
8. **In the Weight field, enter the weight you want.**
9. **In the Description box, enter a description of the model.**
10. **Click Save.**

    The Model Details page for the new model appears.



Editing a Model

You can edit a model's general information and add or delete rules as needed.

To edit a model

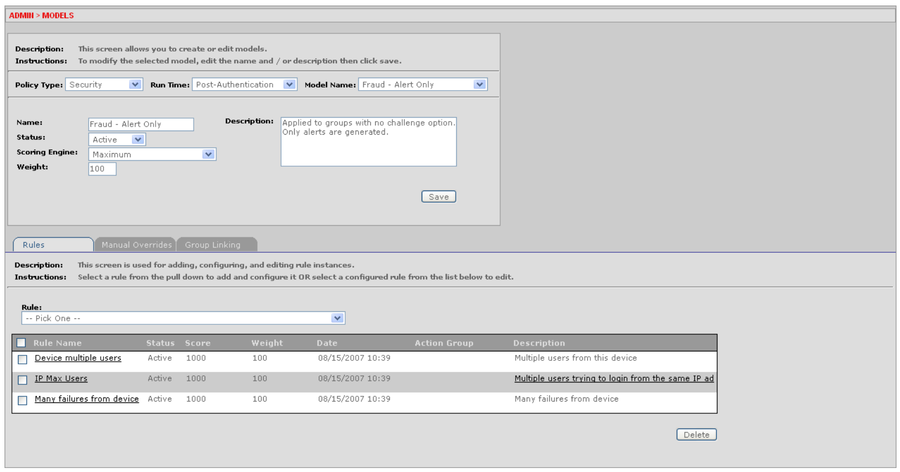
1. **On the Admin menu point to Models and then click List Models.**

   The List Models page appears.

2. **Enter the search criteria you want and click Run Query.**

3. **On the List Models page, click the name of the model you want to edit.**

   The Model Details page appears.



4. **To edit the model's general information, make the changes you want at the top of the page and then click Save.**

   The Model Details page provides tabs to the Rules page, Manual Overrides page, and Group Linking page.

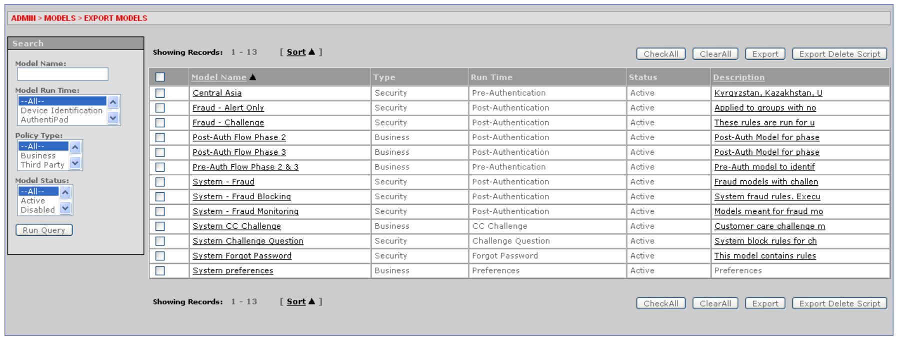
Exporting and Importing a Model

You can use the Export and Import Models commands to export and import a model as an XML file.

To export a model

1. **On the Admin menu, point to Models then click Export Models.**

   The Export Models page appears.



2. **Enter search criteria and click Run Query to locate the model.**
3. **Click the checkbox next to each model you want to export.**
4. **Click Export in the lower right corner of the page.**
5. **Click OK to the confirmation.**

   The Open dialog box appears.

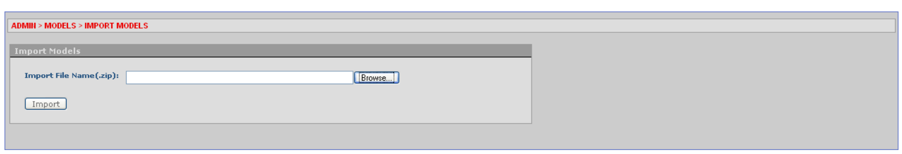
6. **Click Save To Disk and then click OK.**

   The model is exported.

To import a model

1. **Before importing a model all of the groups that the model depends on need to be imported.**
2. **On the Admin menu, point to Models and click Import Models.**

   The Import Models page appears.



3. **Click Browse and locate the model file you want to import.**
4. **Click Import.**

   The model is imported.

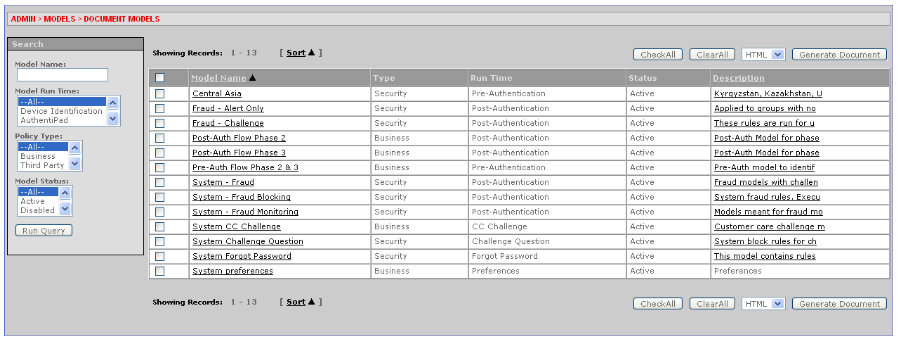
Document Models

The Document Models page allows you to view at a glance the settings of all the rules in a model. You can also print a document containing these settings.

To view the setting of the rules in a model

1. **On the Admin menu, point to Models and click Document Models.**

   The Document Models page appears.



2. **To find a specific model, enter the name of the model in the Model Name field and click Run Query.**
3. **To find models with a specific run time, in the Run Time list, click the run time you want and click Run Query.**
4. **To find models with a specific policy type, in the Policy Type list, click the policy type you want and click Run Query.**
5. **To find models with a specific status, in the Model Status list, click the status you want and click Run Query.**
6. **To print a document of the rule settings in a model, select the model you want, select PDF or HTML, and click Generate Document.**

Policy Sets

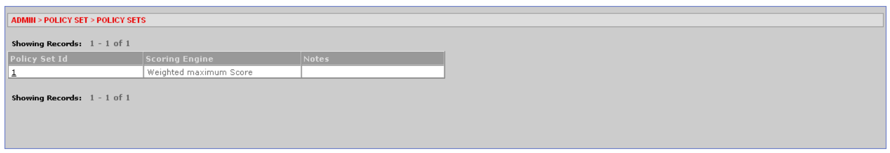
The Policy Sets page displays a list of the policy sets used to evaluate traffic in order to identify possible risks. This page provides access to the Policy details page where you can specify the scoring engine and the weighting you want to use for evaluating risk.

ORACLE ADAPTIVE ACCESS MANAGER uses the scoring engine to calculate the numeric score applied when calculating risk level. It then applies the weight—or multiplier value—to the score to determine its influence on the total score.

To view a list of policy sets

1. **On the Admin menu, point to Policy Sets and then click List Policy Sets.**

   The Policy Sets page appears and displays the Policy Set ID and Scoring Engine for each policy set in the system.



2. **To view details about a policy set, click the Policy Set ID you want.**

To view and edit the policy set details

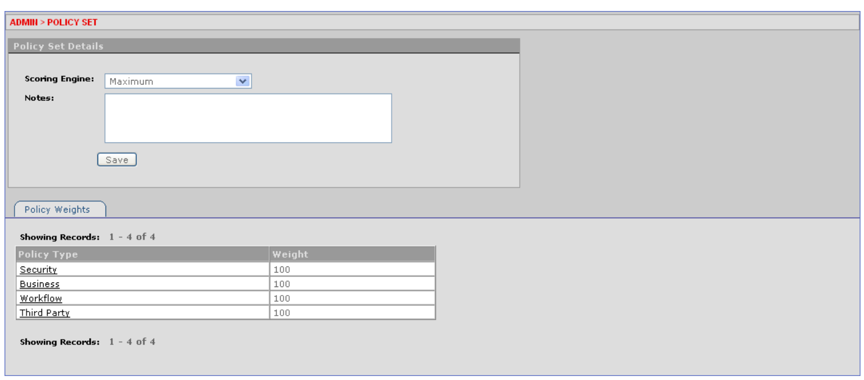
On the policy set details page you can specify the scoring engine used to calculate the score for the policy set that you want to use.

1. **On the Admin menu, point to Policy Sets and then click List Policy Sets.**

   The Policy Sets page appears.

2. **Click the Policy Set ID you want.**

   The Policy Set Details page appears and displays the scoring engine and the policy weights for the Policy Types included in the Policy Set. Each policy type contains all the corresponding models.



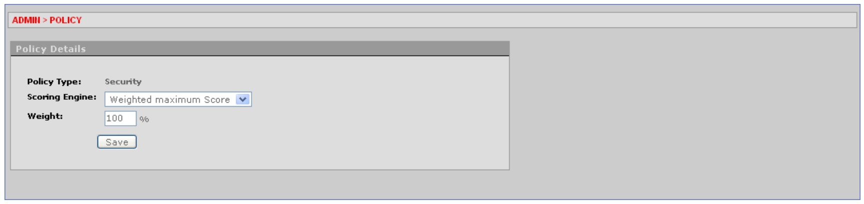
3. **To change the policy weight, in the Scoring Engine list, select the scoring engine you want and click Save.**

To view and edit the policy details for a specific policy type

On the policy details page you can specify the scoring engine used to calculate the score for the policy set and the weighting of this policy against other policies.

1. **On the Policy Set Details page, click the Policy Type you want.**

   The Policy Details page appears.

2. **To change the Scoring Engine, in the Scoring Engine, select the scoring engine you want.**
3. **To change the weight percentage, enter the percentage you want in the Weight field.**
4. **Click Save.**

Adding a New Rule to a Model

To add a rule to a model

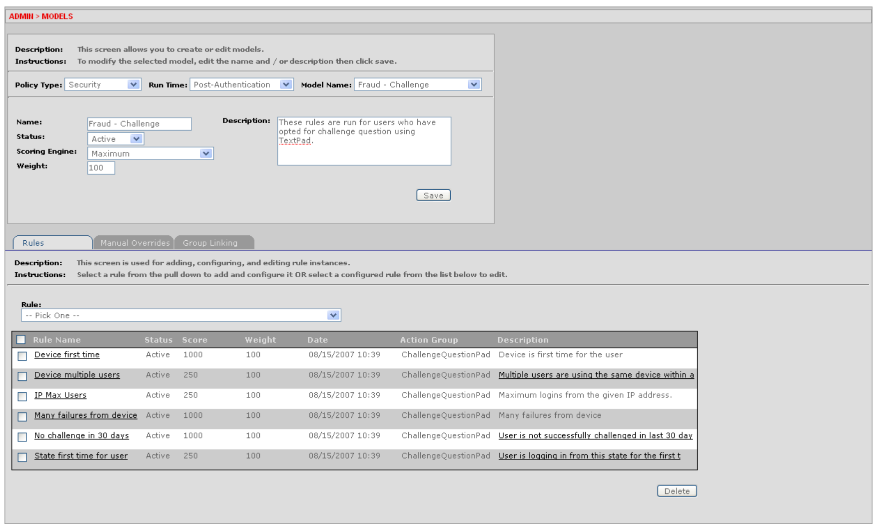
1. **On the Admin menu point to Models and then click List Models.**

   The List Models page appears.

2. **Enter the search criteria you want and click Run Query.**

3. **Click the name of the model you want to edit.**

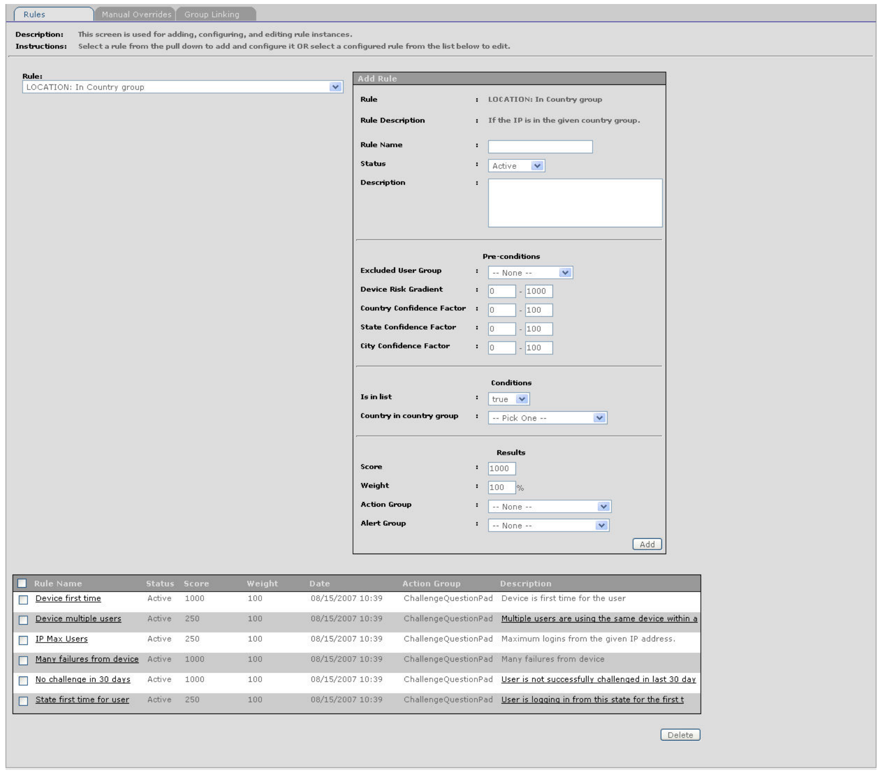
   The Model Details page appears.



4. **In the Rules list, click the name of the rule you want to add.**

   You might, for example, select the rule LOCATION: In Country group. This rule checks whether a country is a member of a specific country group. This rule could be used to black list countries.

   The parameters of the rule appear in the Custom Rule area.



5. **In the Rule Name box, enter the name you want for this instance of the rule template.**

   When you add a rule to a model you are adding an instance of a rule template. You can then customize that instance.

6. **Specify any settings needed for the pre-conditions.**

   These settings determine if the rule will run.

7. **To exclude a user group from the rule, click in the Excluded User Group and select the user group whose members you want this rule to ignore.**

8. **If the rule instance you are configuring is dependent on device identification accuracy, enter a score range for Device Risk Gradient to specify the amount of device identification risk with which you want the run the rule.**

   For example, if the range is 0 to 400, the rule will only run if the device ID is greater than 60% positive.

9. **If the rule instance you are configuring is dependent on IP location identification accuracy, enter a score range for Country, State, and City confidence factors to specify the amount of geo-location accuracy with which you want the run the rule.**

   For example, if the range is 60 to 100 the rule will only run if the IP location is greater than 60% positive. This confidence factor is based on IP geolocation information provided by the IP location vendor.

10. **Specify the threshold values you want for any conditions.**

    For example, enter the group ID or number of seconds elapsed.

11. **In the Actions Group list, select the group of actions you want triggered by this rule, if actions are required.**

12. **In the Alerts Group list, select the group of alerts you want sent if this rule is triggered.**
13. **Enter a rule score and weight value.**

    You can change the weight value for a rule to instruct Adaptive Risk Manager Offline to give more or less value to the total score.
14. **Click Add.**

    Adaptive Risk Manager Offline adds this rule instance to the list of rules in the model.

Customizing a Rule

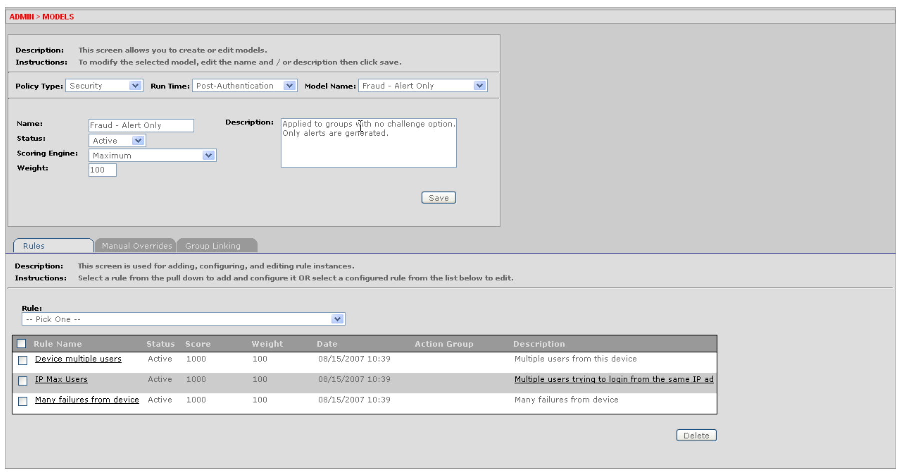
When you add a rule to a model you are not actually adding the rule itself, but rather you are adding an instance of a rule template for which you can edit the parameters.

When you add rules to a model, you select the rule you want to activate and then provide the threshold values. By so doing, you instruct Adaptive Risk Manager Offline to activate a pre-defined set of actions, alerts and/or additional models when the threshold values are exceeded.

To customize a rule

1. **Display the Model Details page for the model you want to edit.**
2. **At the bottom of the page, click the name of the rule you want to edit in the list of rules that have already been added to the model.**

   The parameters of the rule appear in the Custom Rule area.



3. **To change the name, make the change you want in the Rule Name box.**
4. **Specify the threshold values you want for any conditions.**

   For example, specify the group ID, list ID, number of seconds elapsed, or authentication status.
5. **To change the actions group triggered by this rule, select the actions group you want from the Actions Group list.**
6. **To change the alerts group triggered by this rule, select the alerts group you want from the Alerts Group list.**
7. **You can change the weight or score by selecting a different value from the lists.**
8. **Click Save.**

Examples of Customized Rules

Below are some examples of customizing rules.

To activate an action and/or alert if a user is accessing from more than x devices within the specified time:

1. **On the Admin menu point to Models, and then click List Models.**
2. **Enter the search criteria you want and click Run Query.**
3. **On the List Models, click the name of the model you want to edit.**
4. **In the Rules list, select USER: Devices.**

   The parameters for the rule are displayed in the Rule Instance Parameters area.
5. **Click in the Rule Name box and type a name for the rule.**
6. **Click the Max number of devices box and enter a threshold number**
7. **Click in the Duration box and specify the number of seconds you want.**

   For example, you might enter 120 seconds.
8. **Click in the Action box and select the action group you want.**

   For example, you might select an action group that includes Block so that Adaptive Risk Manager Offline will prevent the login attempt.
9. **Click in the Alert box and select the alert group you want.**

   For example, you might select an alert level of High if a user logs in from more than 2 devices within 120 seconds.
10. **Click Save.**

To activate an action and/or alert if the number of users using this device exceeds x for the past x seconds:

1. **On the Admin menu point to Models, and then click List Models.**
2. **On the List Models page, click the name of the model you want to edit.**
3. **In the Rules list, select DEVICE: Multiple Users.**

   The parameters for the rule are displayed in the Rule Instance Parameters area.
4. **Click in the Rule Name box and type a name for the rule.**
5. **Click in the Seconds Elapsed box and type the number of seconds you want.**

   For example, you might enter 120 so that Adaptive Risk Manager Offline will take some action if more than x users use this device in less than 120 seconds.
6. **Click in the Maximum Number of Users Allowed box and type maximum number of users you want.**

   For example, you might enter 2 as the maximum number of allowed users in 120 seconds.
7. **Click in the Action box and select the action group you want.**

   For example, you might select an action group that includes Block.

8. **Click in the Alert box and select the alert group you want.**

   For example, you might select an alert group that includes a High alert.

9. **Click Save.**

To activate an action and/or alert if the number of login attempts with the given client exceeds x for the given time period:

1. **On the Admin menu point to Models, and then click List Models.**
2. **On the List Models page, select the model you want to edit.**
3. **In the Rules list, select USER: Client And Status.**

   The parameters for the rule are displayed in the Rule Instance Parameters area.

4. **Click in the Rule Name box and type a name for the rule.**
5. **Click in the Used Client and select the client you want.**

   For example, you might select PinPad so that if the user enters the pin using a PinPad more than x times for the given period Adaptive Risk Manager Offline will take some specified set of actions.

6. **Click in the More than box and type maximum of attempts.**

   For example, you might enter 5.

7. **Click in the Duration Condition box and type the amount of time you want to evaluate.**

   For example, you might enter 30 minutes as the time in which a user can use the PinPad 5 times before Adaptive Risk Manager Offline takes specified action.

8. **Click in the Action box and select the action group you want.**

   For example, you might select an action group that includes Challenge Questions.

9. **Click in the Alert box and select the alert group you want.**

   For example, you might select an alert group that includes a Medium alert.

10. **Click Save.**

To activate an action and/or alert if the IP is in the given country group:

1. **On the Admin menu point to Models, and then click List Models.**
2. **On the List Models page, click the name of the models you want to edit.**
3. **In the Rules list, select LOCATION: In Country Group.**

   The parameters for the rule are displayed in the Rule Instance Parameters area.

4. **Click in the Rule Name box and type a name for the rule.**
5. **Click in the Group ID box and select the group of counties you want.**

   For example, you might want to select the group of countries that you created from which there have been many fraud attempts in the past three months.

6. **Click in the Action box and select the action group you want.**

   For example, you might select an action group that includes Block.

7. **Click in the Alert box and select the alert group you want.**

For example, you might select an alert group that includes a Medium alert.

8. **Click Save.**

Editing a Model's Links

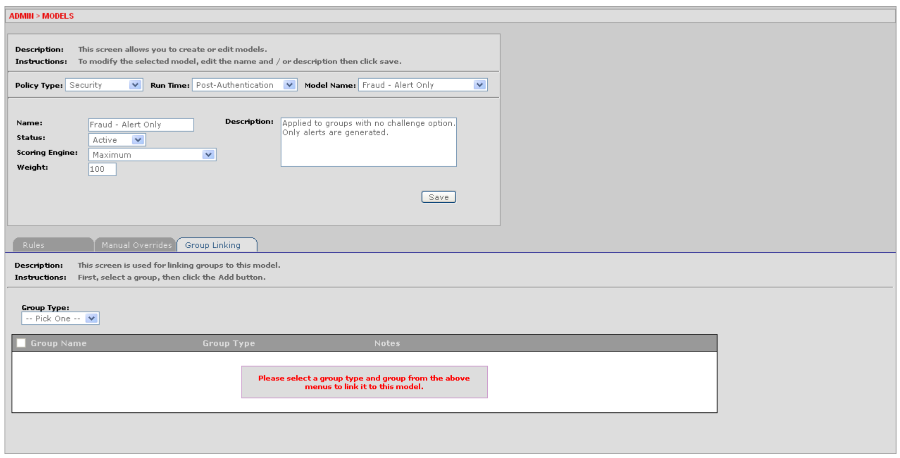
You can add and delete the User ID groups linked to a model as needed. Multiple User ID groups can be linked to a single model if required. If a model's name starts with the word "system" then its rules will apply to all users on the system regardless of group linking.

To edit a model's links

1. **On the Admin menu point to Models, and then click List Models.**
2. **Enter the search criteria you want and click Run Query.**
3. **In the List Models page, click the name of the model you want to edit.**

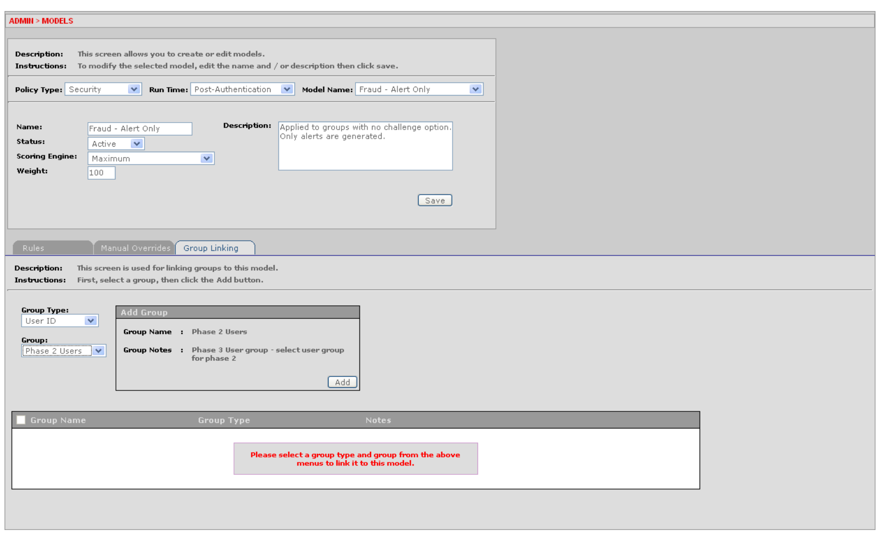
   The Model Details page appears.
4. **Click the Group Linking tab.**

   The Group Linking page appears.



5. **Click in the Group Types box and select the User ID group type.**
6. **Click in the Group Name box and select the group you want to link.**

   The User ID group's details appear in the Add Group area.



7. **Click Add.**

   The new link is added to list of linked User groups.

   To delete a linked group, select the checkbox next to the group you want to delete and then click Delete.

Specifying the Scoring of Rule Return Combinations

ORACLE ADAPTIVE ACCESS MANAGER uses a system of numeric scoring to represent the risk level associated with a specific situation. Each rule has its own default score and weight. Most rules are Boolean and return a value of True or False; they either trigger the rule or they don't. ORACLE ADAPTIVE ACCESS MANAGER uses the score and weight of each rule within a model to calculate the total model risk score.

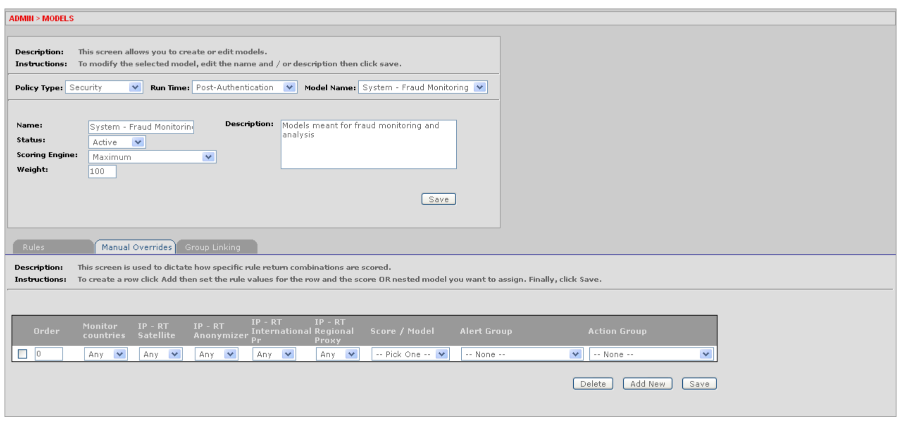
The Manual Overrides page enables you to create outcomes based strictly on the combinations of rule triggers. You can specify a score, action group and alert group based on different rule return combinations or you can point to a nested model to further evaluate the risk. The rows of manual overrides evaluate from top to bottom, stopping as soon as a rule return combination is matches. Actions and alerts triggered by a manual override will be added to any actions and alerts triggered by individual rules.

To specify rule return combinations

1. **On the Admin menu point to Models, and then click List Models.**
2. **Enter the search criteria you want and click Run Query.**
3. **In the List Models page, click the name of the model you want to edit.**

   The Model Details page appears.
4. **Click the Manual Overrides tab in the lower half of the page.**

   The Manual Overrides page appears.



5. **Select the return value permutations you want for each rule in the first row.**
6. **In the Score/Model column, select score or model to specify whether the result should be a score or point to a nested model.**
7. **If you selected Score, in the right-hand column specify the score you want to assign to that combination.**
8. **If you selected Model, in the right-hand column specify the model you want Adaptive Risk Manager Offline to run to further evaluate the risk.**
9. **If you want to specify other rule return combinations, click Add New to add another row.**
10. **Repeat steps 4 through 7 for each rule return combination you want.**
11. **Click Save.**

To delete a rule return combination

1. **Display the Manual Overrides page.**
2. **Select the check to the left of the combination you want to delete and click Delete.**

To change the sequence of a rule return combination

1. **Display the Manual Overrides page.**
2. **To change the numbering sequence of a combination at once, click in the number field and type the new number then click Save.**

Viewing a List of Models

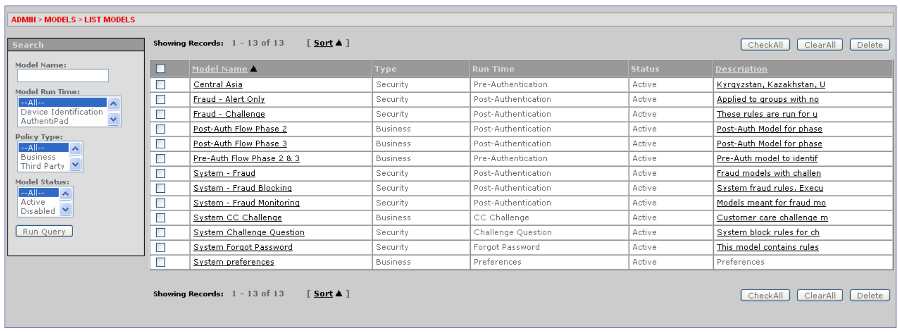
On the List Models page, you can view a list of all models. The List Models page provides quick access to the Model Details page for any model.

To view a list of models

1. **On the Admin menu, point to Models, and then click List Models.**

   The List Models page appears.

2. **Enter the search criteria you want and click Run Query.**



3. **To filter the list by Model Type, select the type you want in the Model Type list and click Submit Query.**

4. **To filter the list by Model Run Time, select the run time you want in the Model Run Time list and click Submit Query.**

5. **To filter the list by status, click status you want in the Model Status list and click Submit Query.**

6. **To find a specific model, type the name of the model in the Model Name box and click Submit Query.**

7. **To view the details page for a model, click the Model Name.**

8. **To delete a model, select the checkbox to the left of the model name and then click Delete. If there are dependent groups you will see a warning message.**

Viewing and Changing Model Details

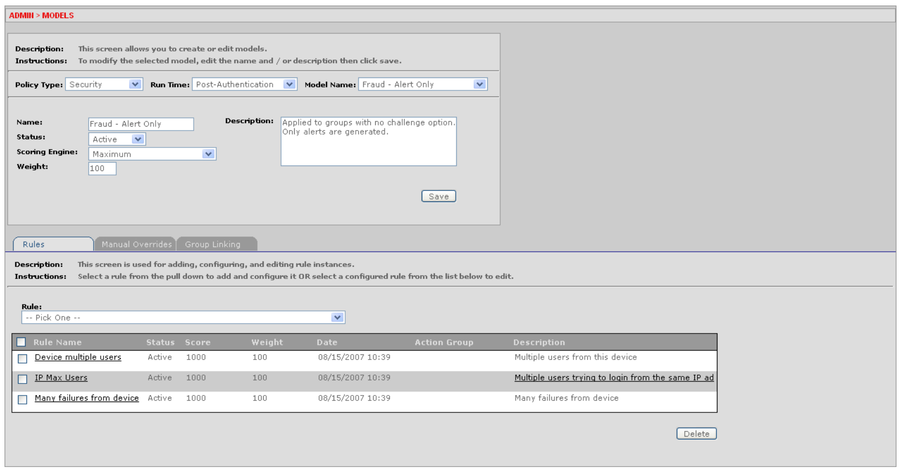
To modify details about a model

1. **On the Admin menu point to Models, and then click List Models.**

   The List Models page appears.

2. **Enter the search criteria you want and click Run Query.**
3. **Click the name of the model you want to view or modify.**

   The Model Details page appears.



4. **To change the model name, click in the Model Name box and type the name you want.**
5. **To change the description, click in the Description box and edit the description.**
6. **Click Save.**

To view details about the user groups linked to a model

1. **On the Admin menu point to Models, and then click List Models.**

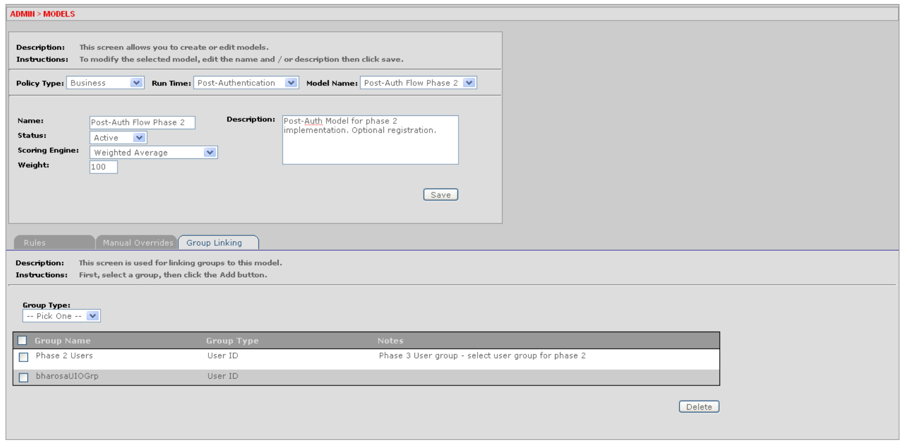
   The List Models page appears.

2. **Enter the search criteria you want and click Run Query.**
3. **Click the name of the model you want.**

   The Model Details page appears.

4. **Click the Group Linking tab.**

   All of the user ID groups linked to the model are listed.



5. **To delete a group, select the checkbox to the left of the group and then click Delete.**

To view details about the rules contained in a model

1. **On the Admin menu point to Models, and then click List Models.**

   The List Models page appears.

2. **Enter search criteria and click Run Query.**

3. **Click the name of the model you want to modify.**

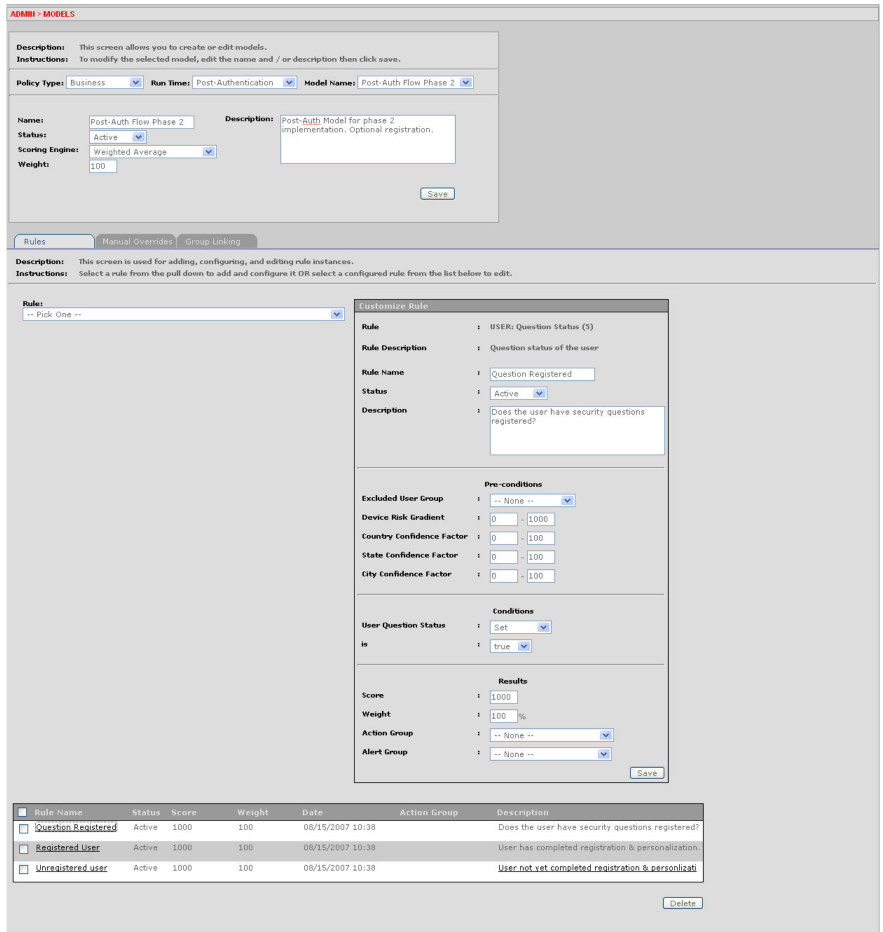
   The Model Details page appears.

4. **Click the Rules tab.**

   The rules contained in the model are listed.

5. **To view the rule details, click the name of the rule you want.**

   The parameters appear in the Custom Rule area.



6. To view the Rule Details page, click the rule you want to see.
7. To view a complete description of the rule, click the link in the Description column.

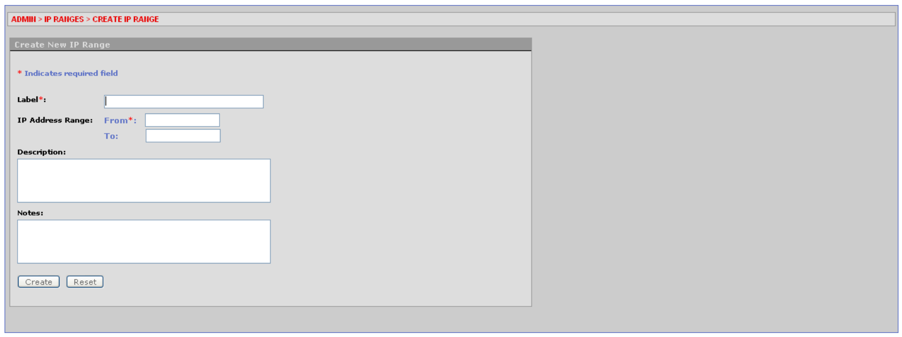
Creating a Group of IP Ranges

You can create a group of IP ranges to use as a parameter in rules. For example, the result of a rule's execution might be to block a user if their IP address falls within a predefined range.

To create a group of IP ranges

1. **On the Admin menu point to IP Range, then click Create IP Range.**

   The Create New IP Range page appears.

2. **Click in the Label box and type a label for the range.**
3. **Click in the From box and type the starting IP range.**
4. **Click in the To box and type the ending IP range.**
5. **Type any description and notes you want.**
6. **Click Create.**

   The IP Range Details page appears.

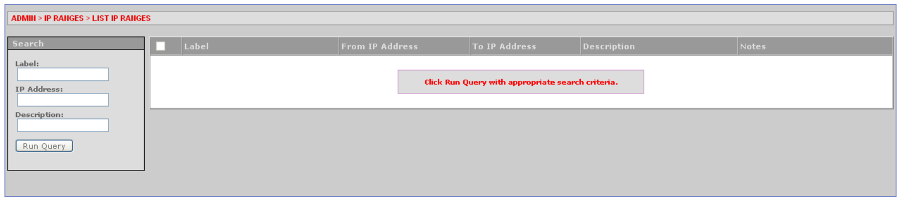
7. **To change the label or IP range, click Modify.**

Viewing a list of IP Ranges

To view a list of IP ranges

1. **On the Admin menu point to IP Ranges, and then click List IP Ranges.**

   The List IP Ranges page appears.



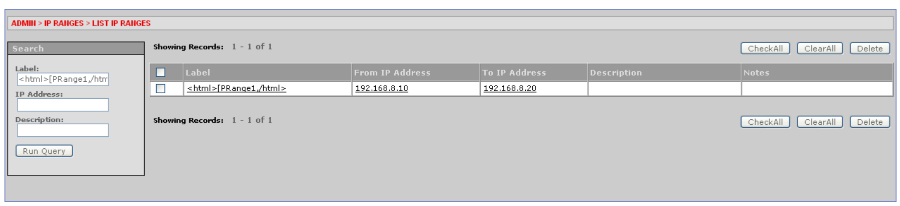
2. **Enter the search criteria you want and click Run Query.**
3. **To view IP range details, click the IP range Label you want.**
4. **To view details about the IP details, click the link in the From or To IP address column.**

To view details about an IP range

1. **On the Admin menu point to IP Ranges, and then click List IP Ranges.**

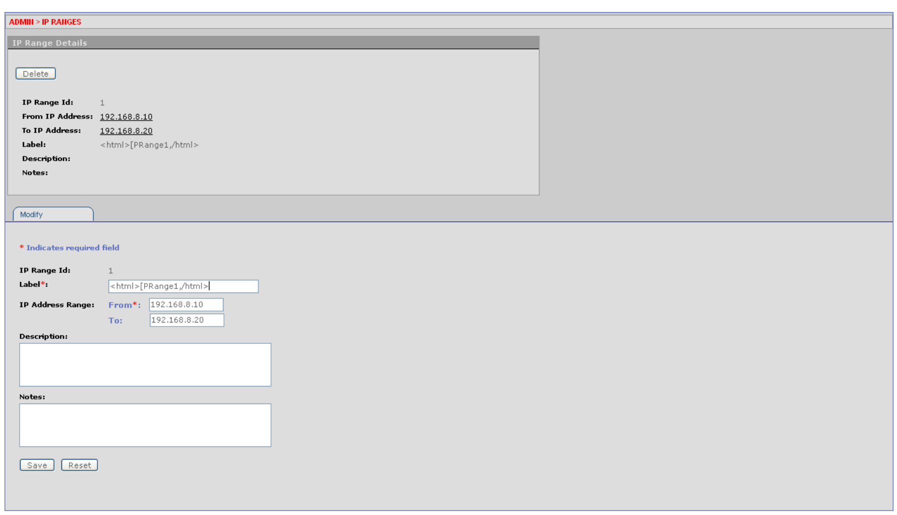
   The List IP Ranges page appears.

2. **Enter search criteria and click Run Query.**



3. **Click the link in the Label column.**

   The IP Details page appears.



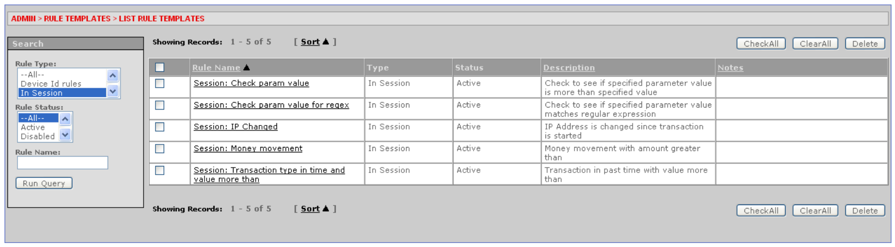
Viewing a List of Rule Templates in the System

To view a list of all the rule templates in the system

1. **On the Admin menu, point to Rules Template and then click List Rule Templates.**

   The List Rule Templates page appears.

   The page displays the list of unconfigured rules.

2. **To filter the list by type, click in the Rule Type box and select the type you want and click Submit Query.**

3. **To filter the list by status, click in the Rule State box and select the status you want and click Submit Query.**

4. **To quickly locate a rule, type the name of the rule in the Rule Name box and click Submit Query.**

5. **To modify the rule description or status, click the rule name.**

6. **To delete a rule, select the checkbox next to the rule name, and then click Delete. Warning, this will completely delete the rule and all its instances from the system.**

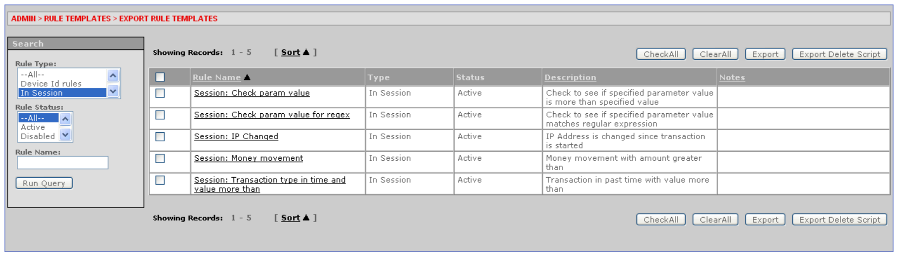
Exporting and Importing a Rule Template

To export a rule template

1. **On the Admin menu, point to Rules Template and then click Export Rule Templates.**

   The Export Rule Templates page appears.

2. **Enter the search criteria you want and click Run Query.**

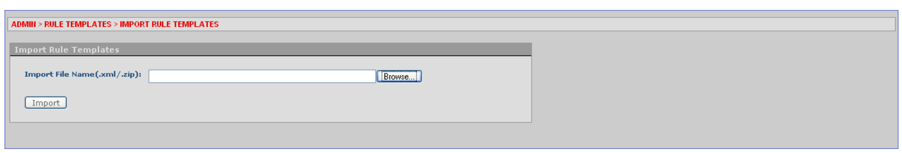


3. **Select the checkbox next to each rule template you want to export.**
4. **Click Export.**
5. **Click OK to the confirmation.**
6. **Click OK to save the rule template to disk.**

To import a rule template

7. **On the Admin menu, point to Rules Template and then click Import Rule Templates.**

   The Import Rule Templates page appears.



8. **Click Browse and locate the rule template you want to import.**
9. **Click Import.**

   The imported template appears in the List of Rule Templates.

Scenarios

This section provides scenarios for setting up and configuring Adaptive Risk Manager Offline to initiate an action in response to different situations.

To create a rule to trigger if more than a set number of users log in from a location in a set amount of time.

1. **Create a model to hold the rule you will add next.**
2. **Add the rule named Location: IP Max Users to the model.**
3. **Configure the seconds elapsed to 30.**
4. **Set max number of users to 3**
5. **Create an *Action* group to be triggered if the rule returns a true result.**
6. **Add the Block Action to the Action Group.**
7. **Link User group and Model.**

To create a rule forcing the system to ask a challenge question the first time a user attempts to log in from a new, unrecognized device

1. **Create a model to hold the rule you will add next.**
2. **Add the rule named Device: Device First Time For User to the model.**
3. **Create an *Action* group to be triggered if the rule returns a true result.**
4. **Add the Question/Answer action to the group.**
5. **Link User Group and Model.**

To create a rule blocking users following a certain number of login failures

1. **Create a model to hold the rule you will add next.**
2. **Add the rule named User: Multiple Failures to the model.**
3. **Configure rule to the maximum number of failed login attempts for a given period of time.**
4. **Create Action group.**
5. **Add the Block action to the group.**
6. **Link User Group and Model.**

Description of Rules

The table below includes a list of rules and rule definitions in the system.

Rule Name	Type	Status	Description
Always On - User	User	Active	This rule always gets processed
Device Id: Cookie state	User Device Id rules	Active	Check the cookie state for the given device and user
Device Id: Cookies Match	Device Id rules	Active	Tracker Node Matches for both cookies.
Device Id: Header data match	Device Id rules	Active	Determines if header data is match
Device Id: Header data match percentage	Device Id rules	Active	Determines if header data match percentage is within specified range.
Device Id: Header data present	Device Id rules	Active	Determines if header data is present
Device Id: Http Header data Browser match	Device Id rules	Active	Determines if Browser is match d based on http header data.
Device Id: Http Header data Browser upgrade	Device Id rules	Active	Determines if Browser is upgraded based on http header data.
Device Id: Http Header data OS match	Device Id rules	Active	Determines if OS match based on http header data
Device Id: Http Header data OS upgrade	Device Id rules	Active	Determines if OS is upgraded based on http header data. Check is based on versions.
Device Id: Is Cookie disabled	Device Id rules	Active	Determines if cookie is disabled for the user based on history.
Device Id: Is Cookie empty	Device Id rules	Active	Determines if cookie value is empty or not empty. Validation check is not included.
Device Id: Is Cookie from same device	Device Id rules	Active	Determines if the http and flash cookies are from same device. Automatically checks old nodes, if current node is not found.
Device Id: Is Cookie Valid	Device Id rules	Active	Determines if there is a valid node for given cookie value.
Device Id: known header data match percentage.	Device Id rules	Active	Determines if known header data match percentage is within specified range.
Device Id: User ASN first time	User Device Id rules	Active	This checks to see if the user has used this ASN successfully previously
Device Id: User Carrier first time	User Device Id rules	Active	This checks to see if the user has used this Carrier successfully previously
Device Id: User IP first time	User Device Id rules	Active	This checks to see if the user has used this IP successfully previously
Device Id: User used this finger print	User Device Id rules	Active	This checks to see if the user has used this fingerprint previously
DEVICE: Browser header substring	Device	Active	Checks whether the supplied string exists as a substring in the browsers header information.

Rule Name	Type	Status	Description
DEVICE: Device in list	Device	Active	Check to see if this device is in list.
DEVICE: Multiple Users	Device	Active	Maximum users using this device for the past x seconds
DEVICE: Timed not status	Device	Active	Maximum login attempts for all but the given status within the given time period.
DEVICE: Used count for User	Device	Active	Device used count
LOCATION: In Country group	Location	Active	If the IP is in the given country group.
LOCATION: In IP group	Location	Active	If the IP is in the IP group.
LOCATION: IP Max Users	Location	Active	Maximum number of users using the current ip address within the given time duration.
LOCATION: IP routing type	Location	Active	Routing type for the IP. It could be fixed/static, anonymizer, AOL, POP, Super POP, Satellite, Cache Proxy, International Proxy, Regional Proxy, Mobile Gateway or Unknown
USER: Account Status	User	Active	Account status of the user
USER: Action Count	User	Active	Checks action counter for the given action.
USER: Authentication Mode	User	Active	Check user authentication mode.
USER: Challenge Channel Failure	User	Active	If a user has a failure counter value over a specified value for more than a specific time from specific channel
USER: Challenge Failure	User	Active	If a user has a failure counter value over a specified value for more than a specific time
USER: Challenge Maximum Failures	User	Active	Check to see if user failed to answer challenge question for specefied number of times.
USER: Challenge timed	User	Active	Check to see if user answered challenge question successfully in last n days.
USER: Question Failure	User	Active	Checks to see how many questions have failures
USER: Question Status	User	Active	Question status of the user
USER: State first time for user	User	Active	Is the user using this State for the first time
WF KBA: Group Date Element After	Device	Active	Check to see if the group date is after current date

Creating a New Database Configuration

Adaptive Risk Manager Offline can be used as a forensic tool in two ways. You can load data directly from the Adaptive Risk Manager Online database or you can load data from a another source database.

Adaptive Risk Manager Offline can also be used as a research and development tool to test new rules on existing data.

The DB Configuration menu enables you to configure the databases you want to run rules against.

If you load data from a foreign source, you need to set up parameters for connecting to the remote database such as URL, password, server type (Oracle driver, SQL server driver, and so on). You also need to configure properties in order to map such fields as the table name, user Id, and browser string.

Adaptive Risk Manager Offline has its own database that has an identical schema to that of the Adaptive Risk Manager Online version. Customer login and/or transaction data must be loaded into the Adaptive Risk Manager Offline database, and Adaptive Risk Manager Offline uses this database to perform risk analysis.

Loading the Data for ARM Offline - Standard Loading Process

Overview

The default implementation for the Adaptive Risk Manager data loader framework works as follows. When in load mode, it uses any configured database as a data source, it expects login data, and it performs device fingerprinting. When in playback mode, it uses the VCRYPT_TRACKER_USERNODE_LOGS and V_FPRINTS tables as its data source, and it runs each record through all active models.

Oracle Adaptive Risk Manager Offline requires login data in the following format:

Required fields

Login_time - The date/time for user when logged into the system

Customer_ID - This field contains information for Customer _ID for the client.

User_ID - This field should contain information for User _ID for the client.

IP_Address - This field contains The IP address from where the client connected.

Browser - This field contains The browser information(Cookie, HTTP Header Information) for the client session.

Auth status - The status of the login attempt - success, wrong password, invalid username, etc.

Optional Fields

Additionally, the following fields are optional.

Device Id - A unique identifier for the users device.

Group Id - Identifies the user group or application

Client Type - Type of the client used by the digital cookie client

Digital Cookie - Digital cookie

Secure Cookie - Secure cookie

To create a new load configuration

1. **On the Admin menu, point to DB Configurations and then click Create Configurations.**

   The Create Configurations page appears.

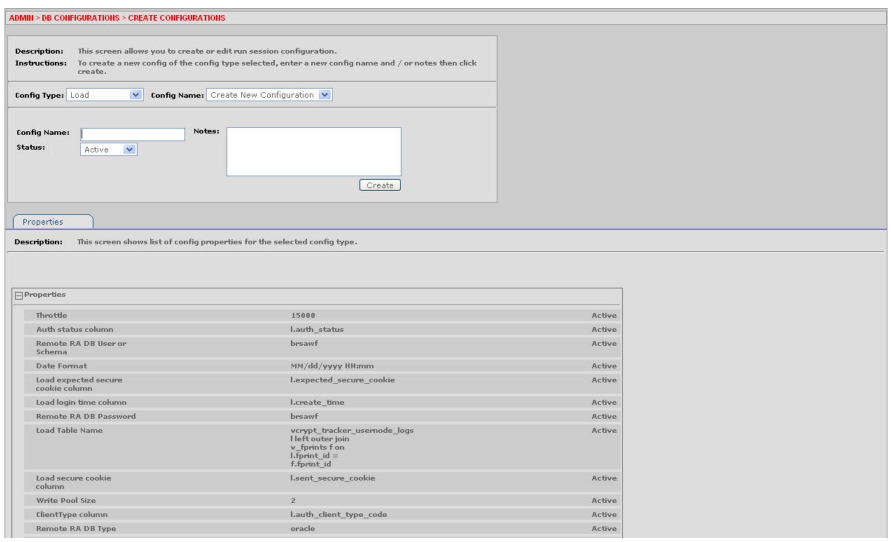
2. **From the Configuration Type menu, select Load.**

3. **From the Configuration Name menu, select Create New Configuration.**

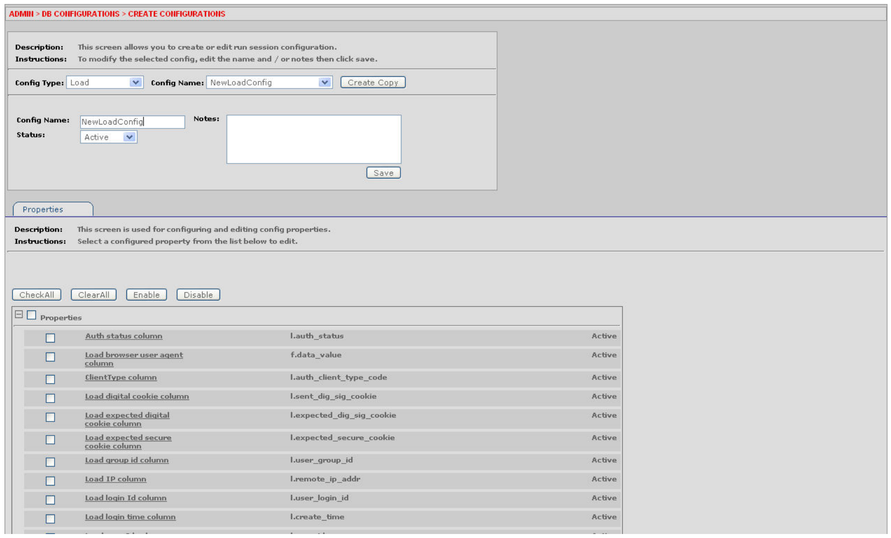
   If you've already created the configuration, you can select from the names of existing configurations.

   The Create New Configurations page appears.

4. **Enter a name for the configuration.**
5. **From the Status menu, select the status you want.**
6. **Enter any appropriate notes.**
7. **Click Create.**

   The properties panel allows you to configure and edit properties.



8. **Review the list of properties at the bottom of the page and modify depending upon the location and structure of your data source.**

   The default values for all of the configuration properties should be correct.

9. **Click Save.**

   If you are loading from an Adaptive Risk Manager Online database, the properties labeled Remote RA DB Type, Remote RA DB Class, Remote RA DB JDBC URL, Remote RA DB User or Schema, and Remote RA DB Password will all need to be changed to the values required to connect to the remote OARM database. The defaults should be correct for all other properties.

   If you are loading from a remote or custom database, you need to set the properties labeled Remote RA DB Type, Remote RA DB Class, Remote RA DB JDBC URL, Remote RA DB User or Schema, and Remote RA DB Password to the required to connect to the custom database.

   Set the value of the property labeled Load Table Name to the name of the table containing the login data. This property value may also include a table alias, e.g. `table t`. If the data is spread across multiple tables, this property can contain join criteria, e.g. `table1 t1 left outer join table2 t2 on t1.id = t2.id`.

   Set the values of the following to the required field expressions.

   - Load login time column
   - Load user Id column
   - Load login Id column
   - Load IP column
   - Load browser user agent column
   - Auth status column
   - Load group id column
   - ClientType column
   - Load secure cookie column
   - Load device id column
   - Load session id column
   - Load expected digital cookie column
   - Load expected secure cookie column

Valid field expressions include database field names (qualified with table aliases if table aliases were specified in the Load Table Name property), e.g. `t1.tstamp` or constants, e.g. `null, 'ra-group'`.

After you create the database configuration, you can begin the process of loading and running data using session sets.

To create a new run configuration

1. **On the Admin menu, point to DB Configurations and then click Create Configurations.**

   The Create Configurations page appears.

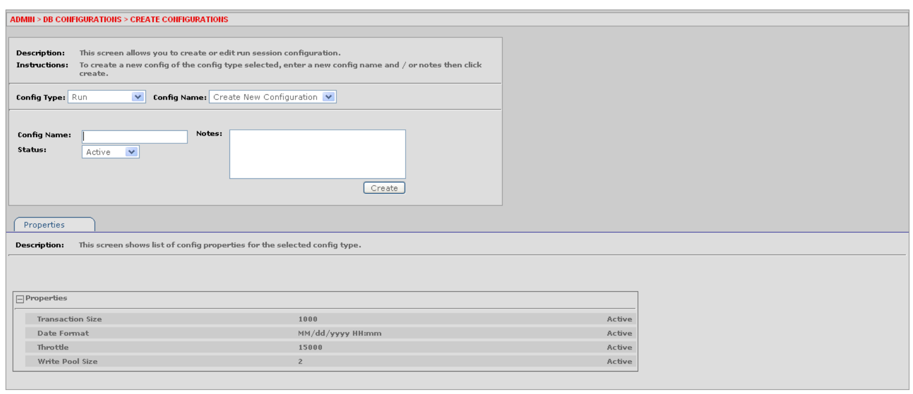
2. **From the Configuration Type menu, select Run.**

3. **From the Configuration Name menu, select Create New Configuration.**

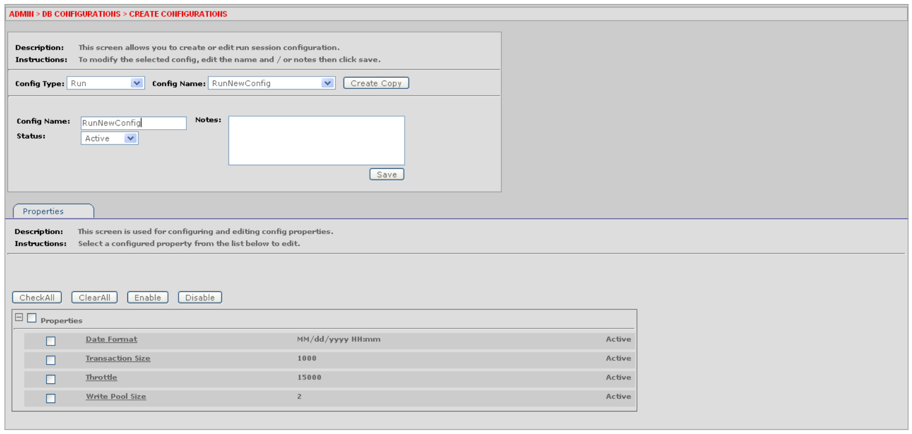
   If you've already created the configuration, you can select from the names of existing configurations.

   The Create New Configurations page appears.

4. **Enter a name for the configuration.**
5. **From the Status menu, select the status you want.**
6. **Enter any appropriate notes.**
7. **Click Create.**

   The properties panel allows you to configure and edit properties.



8. **Review the list of properties at the bottom of the page and modify depending upon the location and structure of your data source.**

9. **Click Save.**

   After you create the database configuration, you can begin the process of loading and running data using session sets.

To view of list of database configurations

1. **On the Admin menu, point to DB Configurations and then click List Configurations.**

   The List Configurations page appears.

2.

3. **To quickly find the configuration you want, enter the name of the configuration.**

4. **To filter the list by configuration type, from the Configuration Type menu, select the type you want.**

5. **To filter the list by status, from the Status menu, select the status you want.**

6. **Click the configuration you want.**

   The Create Configurations page for that configuration appears.

Managing KBA Challenge Questions

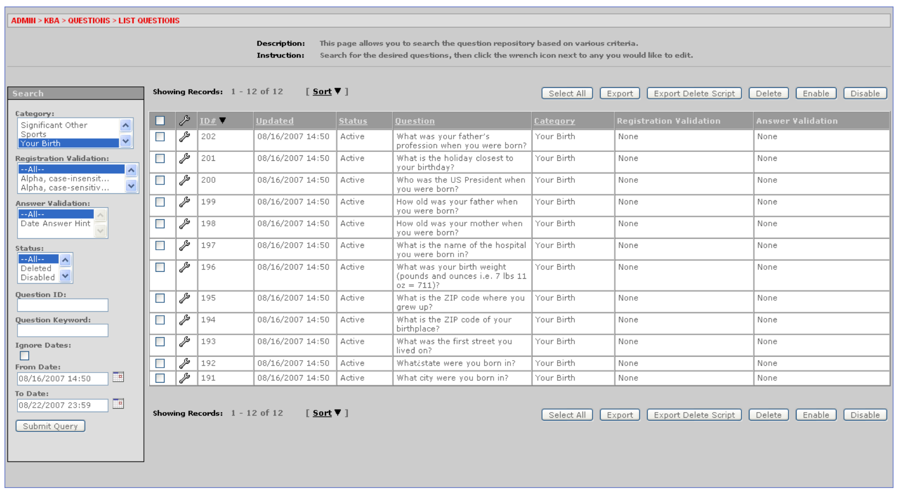
The default KBA configuration presents customers with three question menus. When a customer registers, he or she is required to select one question from each menu. These three questions become the customer's "registered questions". The KBA functionality allows you to manage these challenge questions.

To view a list of all questions

On the List Questions page you can view a list of all challenge questions and search the question repository based on various criteria. The List Questions page provides access to the Questions Details page for any question.

1. **On the Admin menu, point to KBA, point to Questions, and then click List Questions.**

   The List Questions page appears.



2. **To display only the category of questions you want to edit, in the Category list click the category you want and click Submit Query.**

3. **To display only questions with the type of registration validation you want to edit, in the Registration Validation list click the type you want and click Submit Query.**

4. **To display only questions with the type of answer logic hint you want to edit, in the Answer Logic Hint list click the type you want and click Submit Query.**

5. **To display only questions with the status you want to edit, in the Status list click the status you want and click Submit Query.**

6. **To find a specific question, in the Question ID box enter the ID of the question and click Submit Query.**

7. **To find a question by keyword, in the Question Keyword box enter the keyword and click Submit Query.**

8. **To find a question that was created or modified within a specific timeframe, click the calendar icons and select the From Date and To Date you want and click Submit Query.**

9. **To edit a question in the list, click the wrench icon to the left of the question you want to edit.**
10. **To delete, enable, or disable a question, select the checkbox to the left of the question and click the appropriate button above and below the list of questions.**

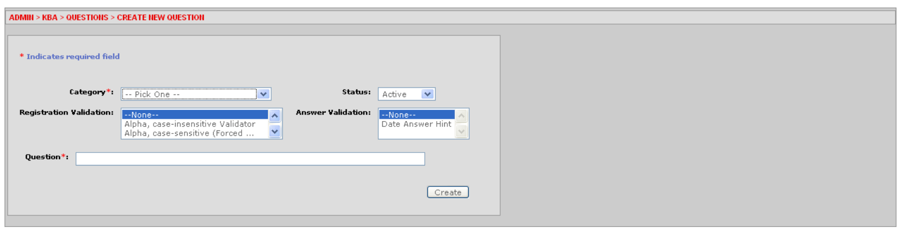
To export questions

1. **On the Admin menu, point to KBA, point to Questions, and then click Export Questions.**
2. **Enter search parameters to find the questions you would like to export.**
3. **Select the questions you want to export then click Export.**

To create a new question

1. **On the Admin menu, point to KBA, point to Questions, and then click Create New Question.**

   The Create New Question page appears.



2. **Type the new question in the question field.**
3. **Click in the Category box and select the category of question you want.**
4. **In the Registration Validation list, click the type of registration Validation you want.**
5. **Click in the Status box and select the status you want.**
6. **In the Answer Logic Hint list, click the type of Answer Logic Hint you want. These hints help the answer logic function more successfully on some questions, date related questions for example.**
7. **Click Create.**

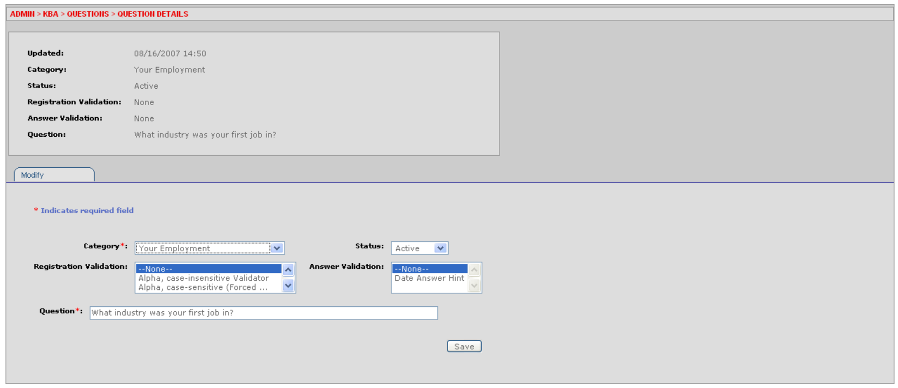
   The Question Detail page appears for the newly created question.

To edit a question

You can activate, disable, and edit a question on the Question Details page. If a question is disabled, customers who have previously selected this question are not affected. If you edit a question, customers using that question will receive the updated question.

1. **On the List Questions page, click the wrench icon next the question you want to edit.**

   The Question Details page appears.

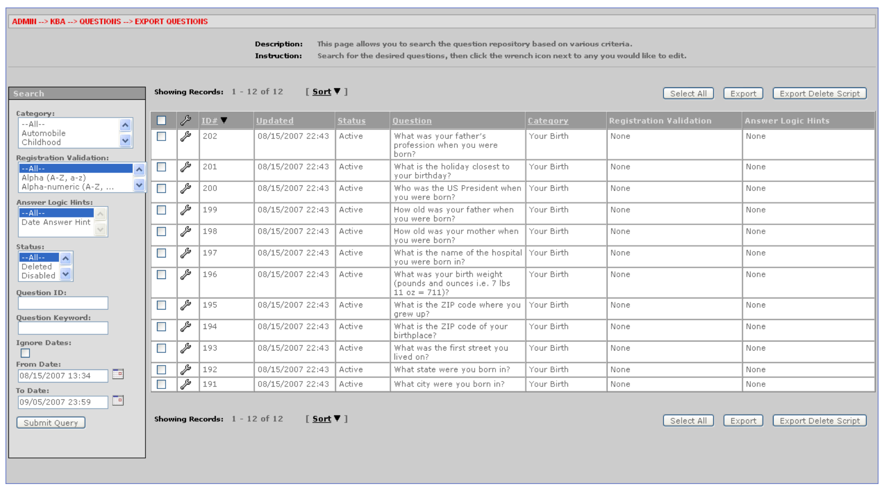


2. **Make the changes you want and click Save.**

To export questions

1. **On the Admin menu, point to KBA, point to Questions, and then click Export Questions.**

   The Export Questions page appears.



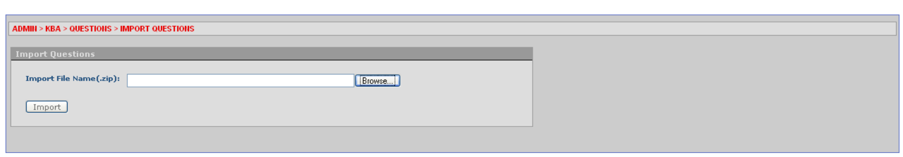
2. **Enter search parameters to find the questions you want to export.**
3. **Select the questions to you want to export and then click Export.**

To import questions

You can import Zip files of questions into the system. If you import questions that belong to a category not currently in the system, the category will also be imported. If you import a question with the same ID# as an existing question, the existing question will be overwritten.

1. **On the Admin menu, point to KBA, point to Questions, and then click Import Questions.**

   The Import Questions page appears.



2. **Click Browse and locate the Zip file of questions you want.**

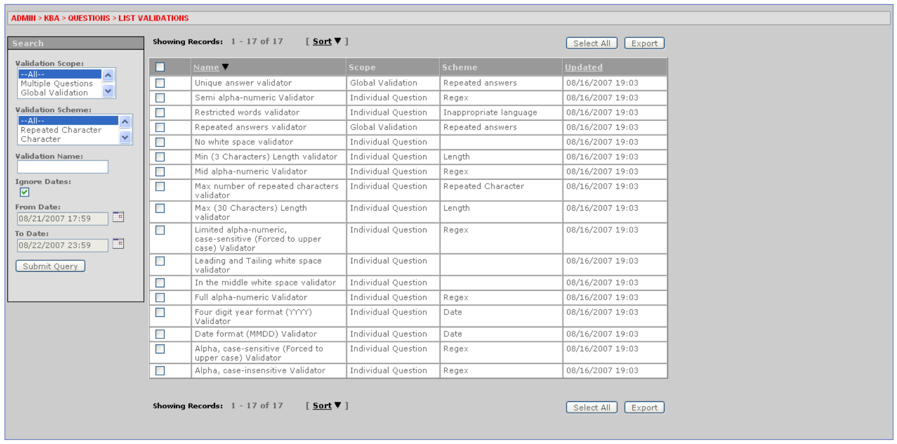
3. **Click Import.**

   The Import Questions page appears with a list of the newly imported questions.

To view a list of validations

1. **On the Admin menu, point to KBA, point to Questions, point to Questions, and then click List Validations.**

   The List Validations page appears.



2. **To display a specific validation scope, in the Validation Scope list, click the scope you want and click Submit Query.**

3. **To display a specific validation scheme, in the Validation Scheme list click the scheme you want and click Submit Query.**

4. **To find a validation, in the Validation Name box enter the name of the validation and click Submit Query.**

5. **To find a validation that was created or modified within a specific timeframe, click the calendar icons and select the From Date and To Date you want and click Submit Query.**

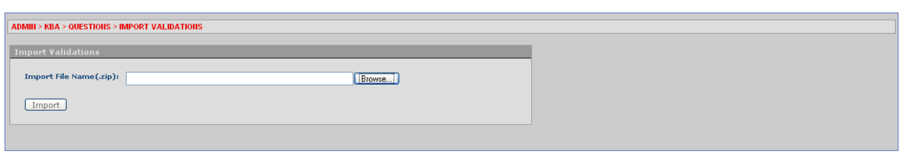
6. **To find all validations regardless of timeframe, select Ignore Dates.**

7. **To Export validations, select the checkbox to the left of the validations you want and click Export.**

To import validations

1. **On the Admin menu, point to KBA, point to Questions, and then click Import Validations.**

   The Import Validations page appears.



2. **Click Browse and locate the Zip file of validations you want.**

3. **Click Import.**

   The Import Validations page appears with a list of the newly imported validations.

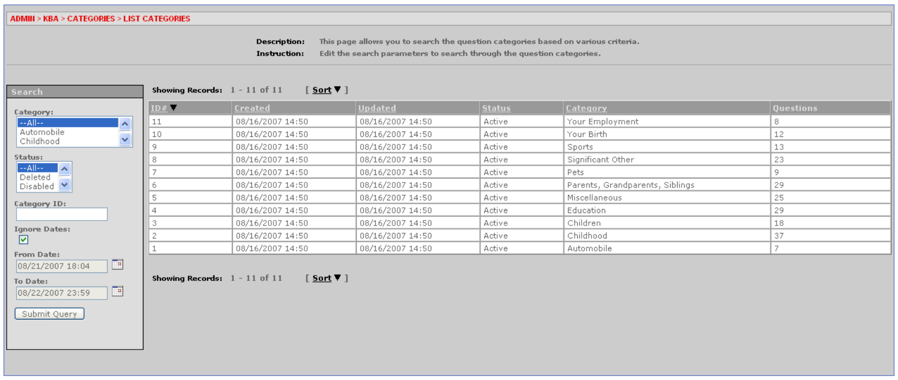
Viewing Categories of Questions

You can search the question categories in the system based on various criteria.

To view question categories

1. **On the Admin menu, point to KBA, point to Categories, and then click List Categories.**

   The Import Categories page appears.



2. **To display a specific question category, in the Category list, click the category you want and click Submit Query.**

3. **To display categories with a specific status, in the Status list click the status you want and click Submit Query.**

4. **To find a specific category, in the Category ID box enter the ID of the category and click Submit Query.**

5. **To find a category that was created or updated within a specific timeframe, click the calendar icons and select the From Date and To Date you want and click Submit Query.**

6. **To find all categories regardless of timeframe, select Ignore Dates.**

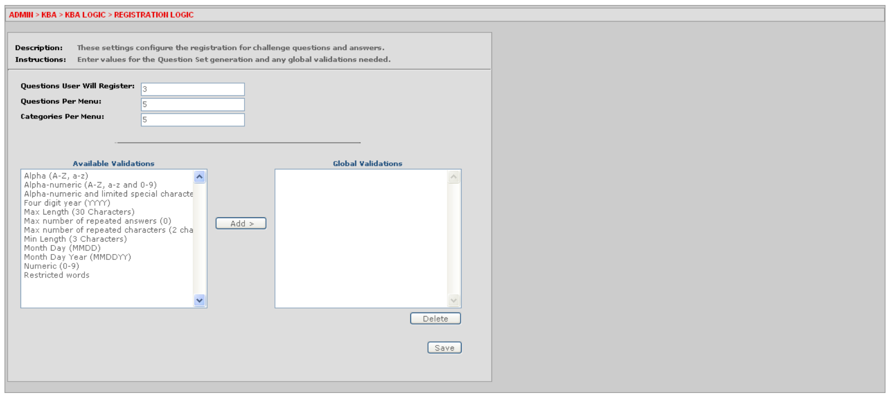
Configuring the Registration Logic

In the Registration Logic area you can manage and configure the registration for challenge questions and answers. To do so, you enter values for the Question Set generation and any global validations needed.

To view and configure the registration for challenge questions and answers

1. **On the Admin menu, point to KBA, point to KBA Logic, and then click Registration Logic.**

   The Registration Logic page appears.

2. **To enter or change the values for the question set generation, enter a value in the appropriate field at the top of the page.**

   You can specify the:

   - Number of questions that a user needs to register
   - Number of questions that appear on each menu
   - The number of categories per menu

3. **To add global validations, in the Available Validations box, click the validation you want to add and then click Add.**

   The validation appears in the Global Validations box.

4. **To delete a global validation, in the Global Validations box, click the validation you want to delete and then click Delete.**

5. **Click Save.**

Configuring the Answer Logic

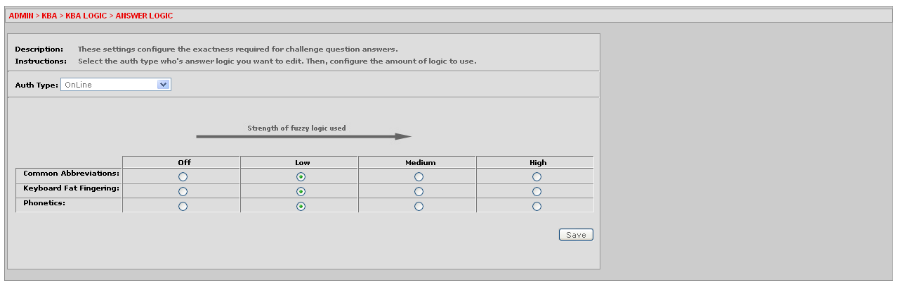
In the Answer Logic area you manage and configure the exactness required for challenge question answers.

To configure the exactness required for challenge question answers

You can configure the answer logic (fuzzy logic) algorithms on the Answer Logic page. The algorithms are divided into three categories: Common Abbreviations, Fat Fingering (accidentally pressing the nearest neighbor on the keyboard), and Phonetics.

1. **On the Admin menu, point to KBA, point to KBA Logic, and then click Answer Logic.**

   The Answer Logic page appears.

2. **Click in the Authentication Type box and specify whether you want the configuration to apply to the Online challenge or CRS Phone Challenge.**

   You can specify different settings for online and phone challenge.

3. **To change the level of answer logic used for a category, select Off, Low, Medium, or High: the lower the setting the higher degree of exactness required.**

4. **Click Save.**

KBA Security Solution Guidelines & Recommended Requirements

These recommendations provide guidelines for implementing KBA authentication. They provide guidance to institutions for configuring and implementing custom enrollment and challenge procedures within the guidelines of best practices.

Questions Guidelines

- No confidential data used in question.
- Answers are difficult to guess.
- Answers cannot be obtained from public sources.
- Questions that are applicable to general public.
- Answers are memorable/personally significant.
- Questions where answers can change over time are avoided.
- Questions cannot pertain to religion, politics, taboo subjects, etc.

Answers Guidelines

- Answers must be at least 4 characters.
- No more than 2 answers can be the same during registration.
- Answers cannot have more than 2 repeating characters.
- Special characters are not allowed.
- Answers are not case sensitive.
- Extra white spaces are removed.
- Fuzzy logic implemented – degree configurable by client.

Business/Security Recommended Requirements

- Unique pick set for each customer.
- Register 3-5 questions. i.e. 15 total questions to select from, 3 drop down menus of 5 questions each.
- Maximum of 2 questions from the same category in a drop-down menu.
- Maximum opt-out – i.e. 3 opt-out attempts before “force” registration.
- When challenged, the same question is to be presented until user responds correctly or question is reset by customer service agent.

Glossary

Action – A response that is triggered by a rule, such as blocking a login after x login attempts within x period of time.

Alert – An alarm or signal that warns an organization to take action to deter potential fraud.

Device – A computer, PDA, cell phone, kiosk, etc.

Group – A collection of users, locations, devices, actions, or alerts.

Location – A city, state, country, IPs, or IP range.

Model – A set of rules that, when linked to a group, are used by Adaptive Risk Manager Offline to evaluate the group member's activity at a specific runtime.

Rule – A rule defines an operation applied by the system to a specified user, device, or location group when a situation is detected that may indicate fraud.

Score – Score refers to the numeric scoring used to evaluate the risk level associated with a specific rule.

Weight – Weight refers to the multiplier value used to influence the total score.

Policy – A policy is a collection of models of the same type.

Policy set – A policy set is the collection of policies used to evaluate traffic in order to identify possible risk.

Index