

Arcot RiskFort™

Administration Guide

Version 2.2.6



455 West Maude Avenue, Sunnyvale, CA 94085

Arcot RiskFort Administration Guide
Version 2.2.6
September 2010
Part Number: RF-0226-00AG-10

Copyright © 2010 Arcot Systems, Inc. All rights reserved.

This guide, as well as the software described herein, is furnished under license and may be used or copied only in accordance with the terms of the license. The content of this guide is furnished for informational purposes only. It is subject to change without notice and should not be construed as a commitment by Arcot Systems.

Arcot Systems makes no warranty of any kind with regard to this guide. This includes, but is not limited to the implied warranties of merchantability, fitness for a particular purpose or non-infringement. Arcot Systems shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Except as permitted by the software license, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior written permission of Arcot Systems, Inc.

Trademarks

Arcot®, ArcotID®, WebFort, and WebFort VAS® are registered trademarks of Arcot Systems, Inc. The Arcot logo™, the Authentication Authority tagline, ArcotID Client™, ArcotOTP™, ProxyFort™, RegFort™, RiskFort™, SignFort™, TransFort™, and Arcot Adapter™ are all trademarks of Arcot Systems, Inc.

All other product or company names may be trademarks of their respective owners.

Patents

This software is protected by United States Patent No. 6,170,058, 6,209,102 and other patents pending.

Arcot Systems, Inc., 455 West Maude Avenue, Sunnyvale, CA 94085

Third Party Software

All the third-party software used by RiskFort and related components is listed in Appendix G, “Third-Party Software Licenses” of the *Arcot RiskFort 2.2.6 Installation and Deployment Guide*.

Contents

- Preface xiii**
 - Intended Audience xiii
 - Information Included in this Guide xiii
 - Related Publications xv
 - Conventions Used in This Book xv
 - Contacting Support xvii
- Chapter 1**
- Overview of the Administration Console. 1**
 - About the Administration Console 1
 - Elements of the Administration Console 2
 - Supported Roles 4
 - Users 5
 - Default Administrative Roles 5
 - Scope of an Administrative Role 7
 - Master Administrator 8
 - Global Administrator 9
 - Organization Administrator 9
 - User Administrator 10
 - Summary of Administrative Privileges 10
 - Custom Roles 14
 - Next Steps: Quick Administration 15
 - For Simple Deployments 15
 - For Complex Deployments 17
- Chapter 2**
- Getting Started 21**
 - Accessing the Administration Console 21
 - Changing Password and Profile Information 23
 - Configuring Administration Console Settings 25
 - Updating UDS Configurations 25

Specifying Global Settings for Organizations	29
Specifying Cache Refresh Settings	31
Specifying Basic Authentication Policy Settings	32
Specifying the Basic Authentication Password Policy	32
Chapter 3	
Working with Custom Roles	35
Understanding Custom Roles	35
Things That You Should Know About Custom Roles	36
Pre-Defined Custom Roles	36
Creating a Custom Role	37
Updating a Custom Role Information	39
Deleting a Custom Role	41
Chapter 4	
Managing RiskFort Server Instances	43
Configuring Server Connectivity	43
Creating Trust Stores	47
Configuring Communication Protocols	48
Configuring SSL Communication (Optional)	52
Refreshing or Shutting Down a Server Instance	52
Refreshing a Server Instance	52
On Windows	53
On UNIX-Based Platforms	53
Restarting a Server Instance	54
On Windows	54
On UNIX-Based Platforms	54
Chapter 5	
Understanding RiskFort Rule Basics	55
Evaluation Rules	56
Out-Of-Box Rules	57
Configurable Built-In Rules	57
Non-Configurable Built-In Rules	58
Add-On Rules	58
Evaluation Callout	59
Scoring Engine	59

Chapter 6**Preparing for Add-On Rules: Working with Rule Types 61**

System-Defined Rule Types	61
Numeric Comparison	63
Combination	63
RiskFort Model	63
Velocity	63
Simple List	64
Mapping (or Derived) List	65
Working with Custom Rule Types	66
Adding New Rule Types	67
Viewing Existing Rule Types	68
Sample Input Definition XML	70

Chapter 7**Managing Global Rule Configurations 73**

Logging in as a Global Administrator	74
Logging Out of the Administration Console	77
Security Recommendations While Using the Administration Console	78
Configuring Rulesets	78
Understanding Rulesets	78
Creating Rulesets	79
Configuring Trusted IP Addresses	81
Adding a Trusted IP Address Range	82
Updating a Trusted IP Address Range	84
Deleting a Trusted IP Address Range	84
Configuring Trusted Aggregators	85
Adding a Trusted Aggregator	86
Updating a Trusted Aggregator	91
Deleting a Trusted Aggregator	93
Configuring Negative IP Addresses	93
Adding or Deleting IP Address Ranges	95
Configuring Negative IP Types	96
Configuring Negative Country List	100
Configuring User Velocity	103
Configuring Device Velocity	106

Configuring Zone Hopping	109
Configuring Miscellaneous Rule Settings	112
Related Concepts	112
User Creation Mode	112
Machine FingerPrint (MFP) Threshold	113
Specifying Miscellaneous Rule Configurations	113
Chapter 8	
Configuring Scoring	117
Understanding RiskFort Scoring	117
Configuring Scoring	118
Migrating to Production	121
Chapter 9	
Configuring Callouts	127
Understanding Callouts	128
Callout Implementation	128
Types of Callouts	130
Evaluation Callout	130
Scoring Callout	131
Configuring Callouts	132
Configuring Evaluation Callout	133
Configuring Scoring Callout	137
Working with the Sample Callout	141
Deploying Sample Callouts	142
On Windows	142
On UNIX-Based Platforms	143
Configuring RiskFort Server to Communicate With Sample Callouts	143
Using the Sample Callout	145
Chapter 10	
Managing Organizations	147
Creating and Activating Organizations	148
Creating Organizations in Arcot Repository	148
Creating Organization in LDAP Repository	152
Searching for Organizations	158
Updating Organization Information	160
Updating the Organization Information	161

Updating RiskFort-Specific Configurations	163
Disabling Organizations	163
Enabling Organizations	164
Activating Organizations in Initial State	165
Deleting Organizations	166
Chapter 11	
Managing Organization-Specific RiskFort Configurations	169
Accessing Organization-Specific RiskFort Configurations	170
Creating Rulesets	173
Assigning Rulesets	173
Using Global Configurations	175
Configuring RiskFort for An Organization	177
Chapter 12	
Working with Add-On Rules	179
Understanding Add-On Rules	180
Data Elements and Operators Used for Building Add-On Rules	182
Data Elements	182
Logical Operators	183
Additional Input Elements Used by Add-On Rules	183
Important Notes Related to Additional Inputs	183
Add-On Rule Examples	184
High Amount Check	184
High User Velocity from Unexpected Locations	185
High Device Velocity from Unexpected Locations	185
Wire Transfers from Unexpected Locations	185
Working with Add-On Rules	185
Deploying an Add-On Rule	186
Editing the Attributes of a Deployed Add-On Rule	187
Deleting a Deployed Add-On Rule	188
Uploading Add-On Rule List Data	189
Uploading (Simple) List Data	189
Uploading Mapping (Derived List) Data	192
Chapter 13	
Managing Administrators	195
Creating Administrators	195

Changing Profile Information for Administrator Accounts	199
Searching Administrators	202
Updating Administrator Account Information	205
Disabling Administrator Accounts	209
Enabling Administrator Accounts	210
Deleting Administrator Accounts	211
Chapter 14	
Managing Users	213
Searching Users	213
Updating User Information	216
Promoting Users to Administrators	218
Disabling User Accounts	221
Enabling User Accounts	222
Deleting User Accounts	223
Chapter 15	
Managing Cases	225
Understanding RiskFort Cases	226
Case Basics	226
Case Management Components	227
Case Queues	229
Queue Server	230
Queue Monitor Thread	230
Case Dispatcher Module	231
Expiry Monitor Thread	232
Case Roles	232
Customer Service Representatives	233
Working on Cases	233
Handling Customer Calls	233
Queue Managers	234
Fraud Analysts	234
Case Role Privilege Summary	235
Case States	236
New	236
Open	236
In Progress	237

On Hold	237
Expired	237
Closed	238
Case State Permissions At a Glance	238
Case Management Workflows	239
Case Generation	239
Case Queuing	240
Case Assignment	240
Case Handling	241
Case Expiry	241
Fraud Analysis	242
Managing the Case Queue	242
Viewing the Status of the Queue	242
Updating the Status of the Queue	244
Analyzing Transactions	246
Step 1: Viewing Transactions Summary	247
Step 2: Viewing Case Details	250
Step 3: Viewing Similar Transactions	255
Viewing Related Transactions	256
Step 4: Marking Transactions for Further Investigation	256
Handling Cases	257
Working on Cases (CSRs)	257
Managing Inbound Customer Calls (CSRs)	262
Generating the Fraud Statistics Report	265
Chapter 16	
Managing Reports	269
Summary of Reports Available to All Administrators	270
Administrator Reports	272
My Activity Report	272
Administrator Activity Report	274
User Activity Report	275
Organization Report	277
RiskFort Reports	279
Risk Evaluation Detail Activity Report	279
Risk Advice Summary Report	284

Trusted IP/Aggregator Report	285
Trusted IP Report	285
Trusted Aggregator Report	286
Negative IP Address Report	287
Negative Country Report	288
Exception User Report	289
Add-On Rules Report	290
Rules Data Report	291
Rules Data Classification Report	292
Case Management Reports	293
Generating Reports	294
Notes for Generating Reports	294
Generating Reports	294
Exporting Reports	295
Chapter 17	
Tools for System Administrators	297
DBUtil: RiskFort Database Tool	297
Set up the Master Key	298
Insert a Database User Name and Password	299
Use Additional DBUtil Options	300
arrfversion: RiskFort Modules Version Display Tool	301
arrfadmin: Server Refresh and Shutdown Tool	302
Before You Use the Tool	303
Using the Tool	303
Configuring the Tool for Two-Way SSL Communication with the Server	305
Step 1: Edit riskfortadminclient.ini	305
Configure the Server Management Protocol	306
arrfserver: RiskFort Server Tool	307
Running the Tool in Interactive Mode	307
arrfupload: Quova Data Upload Tool	308
Before You Use the Tool	309
Using the Tool	310
Appendix A	
RiskFort Logging	313
About the Log Files	313

Installation Log File	314
Transaction Log Files	314
RiskFort Server Log	315
Case Management Server Log File	315
UDS Log File	316
Administration Console Log File	316
Format of the RiskFort Server and Case Management Server Log Files	317
Format of UDS and Administration Console Log Files	318
Supported Severity Levels	319
Sample Entries for Each Log Level	320
FATAL	320
WARNING	320
INFO	320
DETAIL	321
Appendix B	
Glossary	323
Index	327

Preface

The Arcot RiskFort 2.2.6 Administration Guide provides information for setting up and managing Arcot RiskFort 2.2.6 using the Arcot Administration Console. This guide covers information for both Windows and UNIX-based platforms (Solaris SPARC® and Red Hat Enterprise Linux 4.0.)

The screenshots used in this guide use the **Administrator Names** specified in the following table.

Table A-1. Administrators Used in the Screenshots in the Guide

Administrator Name	Administrator Role
MASTERADMIN	Master Administrator
MPARKER	Global Administrator
RLAURIE	Organization Administrator
FANTONY	User Administrator
PRUSH	Queue Manager
RGRAHAM	Fraud Analyst
JHUME	Customer Support Representative (CSR)

Intended Audience

This guide is intended for administrators of Arcot RiskFort. It describes how to use the Administration Console to perform the typical administrative tasks relating to maintaining, provisioning, updating, monitoring performance, and modifying RiskFort configurations.

This guide is intended for users who are experienced with:

- Operating system-based administration
- Applicable Oracle and/or MS SQL databases
- Application server and Web server administration

Information Included in this Guide

This guide is organized in parts as follows:

- [Chapter 1, “Overview of the Administration Console”](#), introduces you to the RiskFort Administration Console interface and management hierarchy.
- [Chapter 2, “Getting Started”](#), describes the basic administrative tasks (such as creating administrators, logging in and out of the Administration Console, changing the administrator password) that must be performed by a Master Administrator to get started with the system. It also discusses the procedures for creating, updating, and deleting administrator accounts.
- [Chapter 3, “Working with Custom Roles”](#), explores the ability of a Master Administrator to create and apply Custom roles in RiskFort.
- [Chapter 4, “Managing RiskFort Server Instances”](#), describes how a Master Administrator can set up and manage RiskFort Server and Case Management Queuing Server instances.
- [Chapter 5, “Understanding RiskFort Rule Basics”](#), explains the basics of RiskFort rules and walks you through the rule categories.
- [Chapter 6, “Preparing for Add-On Rules: Working with Rule Types”](#), describes how a Master Administrator can add Rule Types to support Add-On rules.
- [Chapter 7, “Managing Global Rule Configurations”](#), describes the configurations that a Global Administrator can set at the global level, and that can be inherited by individual organizations configured in the system.
- [Chapter 8, “Configuring Scoring”](#), discusses how to configure RiskFort Scoring as a Global Administrator to meet your organization’s business needs.
- [Chapter 9, “Configuring Callouts”](#), discusses how to configure custom Callouts as a Global Administrator to meet your business needs.
- [Chapter 10, “Managing Organizations”](#), describes how to create, search, activate, enable, disable, or delete organizations as an Organization Administrator in RiskFort. The chapter also walks you through the tasks to manage organization-specific configurations that *cannot* be set at global level.
- [Chapter 11, “Managing Organization-Specific RiskFort Configurations”](#), walks you through the tasks to manage organization-specific configurations as an Organization Administrator that *cannot* be set at global level.
- [Chapter 12, “Working with Add-On Rules”](#), discusses how to configure (as an Organization Administrator) additional business rules to extend RiskFort functionality and to meet your business needs.
- [Chapter 13, “Managing Administrators”](#), describes how to create, search, activate, enable, disable, or delete various administrators in the system.

- [Chapter 14, “Managing Users”](#), describes how to search, activate, enable, disable, or delete end users by using the Administration Console.
- [Chapter 15, “Managing Cases”](#), explains the RiskFort feature called Case Management, the functions performed by Case Management administrators, and the procedure to view and update cases.
- [Chapter 16, “Managing Reports”](#), discusses the reports available to each administrative level and explains the use of these reports.
- [Chapter 17, “Tools for System Administrators”](#), discusses the tools provided by RiskFort that system administrators can use to monitor and manage the system.
- [Appendix A, “RiskFort Logging”](#), covers information about all RiskFort log files, the severity levels recorded in the files, and the format of the entries in these files.
- [Appendix B, “Glossary”](#), lists the key terms used in the guide.

Related Publications

Other related publications include:

<i>Arcot RiskFort 2.2.6 Installation and Deployment Guide</i>	This guide provides information for installing and configuring RiskFort and its components.
<i>Arcot RiskFort 2.2.6 Java Developer's Guide</i>	This guide describes the Java APIs provided by RiskFort and also explains how to use them.
<i>Arcot RiskFort 2.2.6 Quick Installation Guide</i>	This guide provides a summary of the tasks required to install RiskFort.

Conventions Used in This Book

The conventions, formats, and scope of this manual are described in the following paragraphs:

Typographical Conventions

This manual uses the following typographical conventions:

<i>Italic</i>	Emphasis, Guide names
Bold	User input, GUI screen text
Fixed	File and directory names, extensions, Command Prompt, CLI text, code in running text

<i>Italic</i>	Emphasis, Guide names
Fixed Bold	Target file or directory name in the path
Fixed	Command Prompt, CLI text, code
<i>Fixed-Italic</i>	File or directory name that might be different from user to user
Link	Links within the guide, URL links

Formats

This manual uses the following formats to highlight special messages:

	Note: Highlights information of importance or special interest.
	Tip: Highlights a procedure that will save time or resources.
	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.
	Important: Information to know before performing an operation.
	Caution: Makes the user attentive of the possible danger.
	Book: Provides reference to other guides.

Contacting Support

If you need help, contact Arcot Support as follows:

Email	support@arcot.com
Web site	http://www.arcot.com/support/index.html

Chapter 1

Overview of the Administration Console

Arcot Administration Console (referred to as "Administration Console" later in the guide) is a Web-based, operation and system management tool, which provides a consistent, unified interface for managing all Arcot products.

This console offers true *multi-tenant architecture*, which enables you to use a single instance of the console to administer multiple organizations or business units within an enterprise. In this model, each organization or business unit can be set up individually with its own configuration. On the other hand, the Administration Console also provides you with the ability to inherit configuration data from the system level and build only specific configurations for each organization.

This chapter introduces you to the Administration Console interface and the supported administrator hierarchy. It covers the following topics:

- [About the Administration Console](#)
- [Elements of the Administration Console](#)
- [Supported Roles](#)
- [Next Steps: Quick Administration](#)



Note: The recommended desktop screen resolution for Administration Console is 1024 x 768.

About the Administration Console

The Administration Console is a Web browser-based, graphical user interface and is accessible from any supported Web browser with network access to the Server. This console enables you to manage all deployed RiskFort instances, where an *instance* represents a RiskFort Server that is available on a specified port.

You can use the Administration Console to configure RiskFort, to set up users and administrative roles, and complete other administrative operations and configuration tasks, such as:

- Configure communication parameters between the server and other RiskFort components

- Configure RiskFort rules according to you business requirements
- Manage organizations, administrators, and users
- Generate administration, transaction, case management, and configuration reports

The tasks that you are authorized to perform, are displayed on the Administration Console through various tabs. These tasks are based on the user group (or role) that you belong to and the administrative privileges that this role has.

Elements of the Administration Console

A typical Administrative screen can be divided in to the following elements:

- Header
- Main Menu
- Sub Menu
- Tasks
- Body

Figure 1-1 illustrates the placement of these elements in the Administration Console.

Figure 1-1 General Layout of the Administration Console

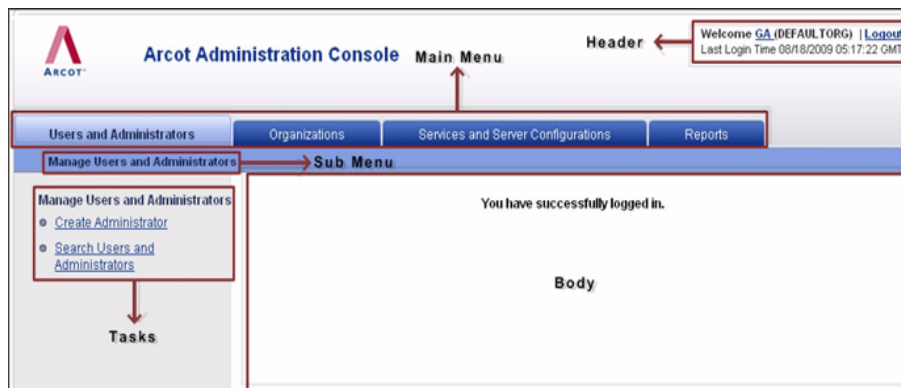


Table 1-1 describes these elements.

Table 1-1. Elements of the Administration Console

Element	Description
Header	Displays login information (administrator name, current organization, the last login date, and time). You can use the links in the header to: • Change the profile information (name, phone number, email ID) and current password. You can also specify the organization that you want to use as a preferred organization for all tasks that you might perform in future. • Log out from the Administration Console.
Main Menu	Displays the main configuration and management options available to the current administrator.
Sub Menu	Displays the options available for the Main Menu item that you clicked.
Tasks	Displays the tasks available for the Sub Menu item that you clicked.
Body	Displays the corresponding page for the selected task.

Console Messages

As shown in Figure 1-2, all the information, warning, and error messages that are generated in the course of using the Administration Console are displayed under the Title of the body page.

While the error messages are displayed in red, as shown in Figure 1-2, the messages indicating success are displayed in blue. Any additional instructions are also a part of these messages, as shown in Figure 1-3.

Figure 1-2 Console Message: Error

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title "Arcot Administration Console" is in the center. On the right, it says "Welcome GA (DEFAULTORG) | Logout" and "Last Login Time 08/17/2009 09:58:04 GMT". Below the header, there are four tabs: "Users and Administrators", "Organizations" (which is selected), "Services and Server Configurations", and "Reports". Under the "Organizations" tab, there is a sub-section "Manage Organizations" with two links: "Create Organization" and "Search Organization". The "Search Organization" link is active. The main content area is titled "Search Organization" and contains a text input field with the placeholder text "Enter the (full or partial) Display Name of the organization that you want to search." Below the input field, a red-bordered box contains the message "The search did not yield any results." followed by a red arrow pointing to the text "Console Error Message". Below this, there is a table with columns: "Organization", "Initial", "Active", "Inactive", and "Deleted". The "Inactive" column has a checked checkbox. There is a "Search" button to the right of the table.

Figure 1-3 Console Message: Success

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the user is logged in as 'GA (DEFAULTORG)' with a 'Logout' link and a last login time of '08/17/2009 09:58:04 GMT'. The main navigation bar includes 'Users and Administrators', 'Organizations' (selected), 'Services and Server Configurations', and 'Reports'. Below this, the 'Manage Organizations' section is active, showing a sidebar with 'Manage Organizations', 'Create Organization' (highlighted with a green dot), and 'Search Organization'. The main content area is titled 'Create Organization' and contains a success message in a red-bordered box: 'Successfully activated the organization, Arcot Systems. You must refresh the cache of each Arcot Product for this change to take effect.' An arrow points from this message to the text 'Console Success Message'. Below the message is a form for creating an organization, with fields for 'Organization Name', 'Display Name', 'Description', 'Administrator Authentication Mechanism' (set to 'Basic User Password'), 'User Data Location', and 'Repository Type' (set to 'Arcot Database'). A 'Create' button is at the bottom of the form.

Supported Roles

Roles enable you to specify which operations and privileges are assigned to a user or a set of users who share similar responsibilities. When a user is assigned to a specific role, the set of functions called *tasks* that are associated to that role become available to the user. As a result, administrators can exercise fine-grain control on the tasks assigned to each user in the system.

The Arcot Administration Console provides you flexibility to set up your administration hierarchy and assign rights to the administrators. You can create different levels of administrators, each with varying degrees of access. You can also create administrators that can, in turn, delegate administration tasks to other users.

The Administration Console supports the following types of roles:

- [Users](#)

- [Default Administrative Roles](#)
- [Custom Roles](#)

Users

Every end user of your online application system is referred to as a *user* in Arcot Administration Console. This user can either exist in your Lightweight Directory Access Protocol (LDAP) repository or in the Arcot database.

If the user already exists in your LDAP system, then you need to map the organization LDAP attributes to Arcot supported attributes. See [“Creating Organization in LDAP Repository” in Chapter 10](#) for more information on how to do this.

To enroll the users in RiskFort database, select the organization whose repository type is Arcot Database. See [“Creating Organizations in Arcot Repository” in Chapter 10](#) for more information on how to do this.

Default Administrative Roles

The Administration Console is shipped with an out-of-the-box administrative user called the [Master Administrator](#) who can perform high-level configurations. Other than this, you must assign users to administrative roles to administer the RiskFort system or to access business data. An administrative role typically comprises a set of privileges based on a job function profile and the scope in which these permissions are applicable. The users with administrative privileges are referred to as *administrative users*.



Note: See [“Summary of Administrative Privileges”](#) for a comprehensive list of privileges available to the each administrative role.

The Administration Console supports the following pre-defined administrative roles:

- [Master Administrator](#)
- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

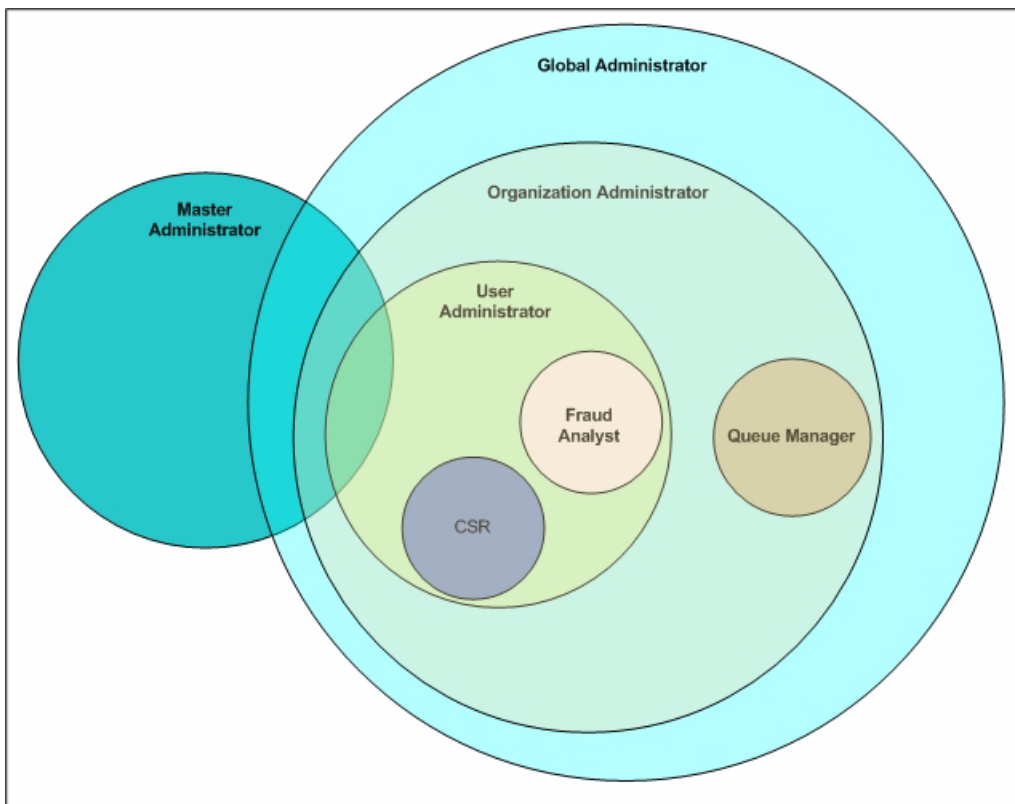
In addition, you can also create [Custom Roles](#).



Note: The administrators are also considered as users of the system.

Figure 1-4 depicts these administrative roles and the relationships between the privileges available to these roles. The sections following the figure discuss the supported administrator levels in details.

Figure 1-4 Administrative Roles and the Relationship Between These Roles



Note: As can be seen in Figure 1-4, the hierarchical distribution of privileges does not allow the administrators to access beyond their fixed boundaries. Each level has a pre-defined privilege or role.

Scope of an Administrative Role

The *scope* of an administrative role in the Arcot Administration Console consists of:

- All the organizations that an administrator with a specific role can manage.
- The privileges associated with the role.

Important Notes About Scope

While creating an administrative role, you must remember that:

- The scope of the **Master Administrator** is **All Organizations** by default, and this administrator manages *all* existing and other organizations that will be created in the future.
- A role (**Global Administrator**, **Organization Administrator**, or **User Administrator**) can only manage down the administrative hierarchy, never up. In other words, a role that manages a child role is defined such that it does not manage the child's parent.

For example, a Global Administrator can manage other Global Administrators with lower scope, Organization Administrators, and User Administrators. However, they *cannot* manage an Master Administrator.

- The scope of a **Global Administrator** role *can* be defined as All Organizations, in which case the role can manage all existing as well as future organizations.
- An **Organization Administrator** or a **User Administrator** role can be limited to manage only specific organizations.
- If the administrator is derived by using **Custom Roles**, then the derived administrator belongs to the same level as that of the parent level.

For example, if you derive an administrator *MyGlobalAdmin* from Global Administrator, then *MyGlobalAdmin* is considered to be a Global Administrator, even though you might have assigned *MyGlobalAdmin* less number of privileges compared to an Organization Administrator or User Administrator.



Note: An **Organization Administrator** or a **User Administrator** role *should not* be defined with the scope as All Organizations.

Master Administrator

The Master Administrator (MA) is the super user of the system, who has unrestricted access to the whole system. The default scope of an MA is All Organizations, as a result of which they can manage all the existing organizations as well as those organizations that will be created by them or any other administrator in the future.

The primary responsibilities of an MA are to:

- Bootstrap (or initialize) the system after installation.
- Configure the User Data Service (UDS) connection parameters.
- Configure the global organizations settings and cache refresh settings for the Administration Console.
- Configure the RiskFort Server communication parameters.
- Configure the RiskFort Server protocol settings.
- Configure the authentication mechanism for the Administration Console and Server components and other miscellaneous settings.
- Create and manage organizations, if required.
- Create and manage administrators of any role (Global, Organization, or User Administrator), as required.
- Manage [Custom Roles](#).

At the end of a successful deployment of Administration Console, you must log in for the first time as an MA. The MA account ([masteradmin](#)) is shipped with a default password ([master1234!](#)). Because the actions of an MA can affect the security of the entire system, Arcot strongly recommends that you change this password after you log in to the console for the first time. Arcot also recommends that you safeguard this password and change it regularly.



Note: In case if the MA account is locked, then you must contact Arcot Technical Support at support@arcot.com.

To track and analyze data, an MA can not only generate a comprehensive report of all their activities, but also generate a report for the activities of other administrators in the system. In addition, they can also generate reports for all organizations and reports for all server configurations.

Global Administrator

The Global Administrator (GA) is the second level in the administrative hierarchy. These administrators can perform most of the tasks of an MA, except for bootstrapping the system, performing initial Administration Console configurations, specifying server configurations, and managing custom roles.

Typically when you create a GA, you need to specify the scope of their administration. Unless you do so, they cannot manage any organization.

The main tasks of a GA are to:

- Create and manage other Global, Organization, or User Administrators, as required.
- Configure the authentication policy for the Administration Console.
- Create and manage organizations, as required.



Note: This includes editing the organization details.

- Manage user credentials.
- Configure RiskFort rules and scoring.
- Assign configurations.
- Configure callouts and Add-On rules.

To track and analyze the available information, GAs can generate and view all administrative activity, configuration, and case management reports for the organizations under their administrative purview. They can also view the reports for all the Organization and User Administrators assigned to them.

Organization Administrator

The Organization Administrator (OA) is the third level in the administrative hierarchy. These administrators can perform all tasks related to management of the organizations assigned to them either by the MA or a GA and the users that belong to the organizations. These tasks include:

- Creating and managing other Organization or User Administrators, as required.
- Managing organizations in their purview.
- Configure the authentication policy for the Administration Console.

- Managing (updating) organization-specific configurations.
- Managing the users that belong to the organizations in their purview.

When you create an OA, you need to specify the scope of their administration. Unless you do so, they cannot manage any organization.

OAs can generate and view administrative activity, configuration, and transaction reports for the organizations under their administrative purview. They can also view the reports for all the User Administrators assigned to them.

User Administrator

The User Administrator (UA) role is the lowest level in the administrative hierarchy. These administrators can perform all tasks related to user management for the organizations assigned to them either by the MA or a GA. These include:

- Creating and managing other UAs, as required.
- Managing users, as required, for the organizations under their purview.



Note: This includes editing the user details.

- Managing end user cases.

When you create a UA, you need to specify the scope of their administration. Unless you do so, they cannot manage any organization.

UAs can generate and view user and UA activity reports for the organizations under their administrative purview.

Summary of Administrative Privileges

[Table 1-2](#) summarizes the privileges available to the supported three levels of administrators.

The column name acronyms used in the table are:

- Master Administrator → **MA**
- Global Administrator → **GA**
- Organization Administrator → **OA**
- User Administrator → **UA**



Note: The ✓ sign indicates the actions (or privileges) that are available to the specified level of administrator.

Table 1-2. Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
User Data Service (UDS) Management	Update Global User Data Service (UDS) Configuration	✓			
Default Organization Management	Configure Default Organization	✓			
Cache Management	Update Cache Refresh Configuration	✓			
Authentication Policy Management	Update the Basic Authentication Policy	✓	✓	✓	
System Configuration Management	RiskFort Connectivity	✓			
	Trusted Certificate Authority	✓			
	Protocol Configuration	✓			
Add-On Rule Management	Add Rule Type	✓			
	View Existing Rule Types	✓			
Custom Role Management	Create Custom Roles	✓			
	Update Custom Roles	✓			
	Delete Custom Roles	✓			
Global Administrator Account Management	Create Global Administrator Accounts	✓	✓		
	Search or View Global Administrator Details	✓	✓		✓
	Update Global Administrator Account Information	✓	✓		✓
	Enable Global Administrator Accounts	✓	✓		
	Disable Global Administrator Accounts	✓	✓		
	Delete Global Administrator Accounts	✓	✓		

Table 1-2. Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
Organization Administrator Account Management	Create Organization Administrator Accounts	✓	✓	✓	
	Search or View Organization Administrator Details	✓	✓	✓	✓
	Update Organization Administrator Account Information	✓	✓	✓	✓
	Enable Organization Administrator Accounts	✓	✓	✓	
	Disable Organization Administrator Accounts	✓	✓	✓	
	Delete Organization Administrator Accounts	✓	✓	✓	
User Administrator Account Management	Create User Administrator Accounts	✓	✓	✓	
	Search or View User Administrator Details	✓	✓	✓	✓
	Update User Administrator Account Information	✓	✓	✓	✓
	Enable User Administrator Accounts	✓	✓	✓	✓
	Disable User Administrator Accounts	✓	✓	✓	✓
	Delete User Administrator Accounts	✓	✓	✓	
Organization Management	Create Organizations	✓	✓		
	Search and View Organization Details	✓	✓	✓	✓
	Update Organization Information	✓	✓	✓	
	Activate Organizations	✓	✓	✓	✓
	Deactivate Organizations	✓	✓	✓	✓
	Delete Organizations	✓	✓		

Table 1-2. Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
User Management	Search and View User Details	✓	✓	✓	✓
	Update User Information	✓	✓	✓	✓
	Activate Users	✓	✓	✓	✓
	Deactivate Users	✓	✓	✓	✓
	Delete Users	✓	✓	✓	✓
RiskFort Configurations	Create Ruleset		✓	✓	
	Assign Ruleset		✓	✓	
	Negative IP Address List		✓	✓	
	Negative IP Types		✓	✓	
	Negative Country List		✓	✓	
	Trusted IP/Aggregator		✓	✓	
	User Velocity		✓	✓	
	Device Velocity		✓	✓	
	Zone Hopping		✓	✓	
	Add-On Rule Configuration		✓	✓	
	Callouts Configuration		✓	✓	
	User Creation Mode		✓	✓	
	Machine FingerPrint (MFP) Threshold Tolerance		✓	✓	
	Scoring Configuration		✓	✓	
	Migrate to Production		✓	✓	
Case Management	Work on Cases		✓	✓	✓
	Manage Inbound Calls		✓	✓	✓
	Analyze Transactions		✓	✓	
	Fraud Statistics Report		✓	✓	
	View Queues		✓	✓	
	Manage Queues		✓	✓	

Table 1-2. Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
Reports	My Activity Report	✓	✓	✓	✓
	Administrator Activity Report	✓	✓	✓	✓
	User Activity Report		✓	✓	✓
	Organization Report	✓	✓	✓	
	Risk Evaluation Detail Activity Report		✓	✓	✓
	Risk Advice Summary Report		✓	✓	✓
	Trusted IP/Aggregator Report		✓	✓	
	Negative IP Report		✓	✓	
	Negative Country Report		✓	✓	
	Exception User Report		✓	✓	✓
	Add-On Rules Report		✓	✓	
	Rules Data Report		✓	✓	
	Rules Data Classification Report		✓	✓	

Custom Roles

As MA, you can also create new administrative roles that inherit a subset of privileges from one of the following pre-defined parent roles:

- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

These roles are called *custom roles*, and are derived by **disabling** some of the default privileges associated with the parent role. For example if you need to disable the "Organization Creation Privilege" for a GA, then you can create a Custom role by disabling this privilege.

If you create a Custom role, then it becomes available as a role option when you create or update an administrative account. In addition to creating custom roles, you can also update and delete them.

In addition to the custom roles that you can create, RiskFort is also shipped with three pre-defined custom roles (as shown in [Figure 1-4](#)) that are required for Case Management. These role include:

- **QM:** The **Queue Manager** role is shipped with the required privileges to supervise cases.
- **CSR:** The **Customer Support Representative** role is shipped with the required privileges to work on cases and attend inbound calls from the end users, if required.
- **FA:** The **Fraud Analyst** role is shipped with the required privileges to analyze cases to find hidden trends and patterns.

See [Chapter 3, “Working with Custom Roles”](#) for more information on working with these custom roles. See [Chapter 15, “Managing Cases”](#) for more information on Case Management.

Next Steps: Quick Administration

Now that you are familiar with the RiskFort Administration Console concepts, this section quickly walks you through the steps for getting ready for administering your deployment. For this purpose, it provides a quick overview for the following scenarios:

- [For Simple Deployments](#)
- [For Complex Deployments](#)

For Simple Deployments

The simplest implementation of RiskFort typically provides adaptive authentication for a small user base. It consists of all the RiskFort components and Web applications installed on a single system. The database can be on the same system where RiskFort is installed, or on a different system.



Book: See Chapter 2, "Planning the Deployment" in the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information on this type of deployments.

[Table 1-3](#) summarizes the typical characteristics of this deployment type.

Table 1-3. Characteristics of Simple Deployments

Characteristic	Details
Deployment Type	• Development, proof of concept, initial testing, or initial pilot • Small to medium businesses (SMBs) • Regional deployment within an enterprise

Table 1-3. Characteristics of Simple Deployments

Characteristic	Details
Geographic Expanse	Typically restricted to a single location
Deployment Requirements	Ease of implementation and management

In case of small deployments, most of the default settings will work out of the box. Because this is a single-organization system, you can use the Default Organization, which is created automatically, when you initialize the system instead of setting up a new organization. As a result, you might not need OA accounts either. You, then, only need to create the required GA and UA accounts.



Note: You can create the end users in RiskFort by using the SDKs that are shipped with the system.

See the Javadocs shipped with the SDKs and this topic will be covered in detail in *Arcot RiskFort 2.2.6 Developer's Guide*.

The **quick overview** of the steps to set up and start managing strong authentication for your users is:

1. Ensure that RiskFort is installed and configured properly and that you have deployed the WAR files for the Administration Console and User Data Service.



Book: See Chapter 4, "Deploying RiskFort on a Single System" in the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information on installing RiskFort, deploying the WAR files, and performing other post-installation tasks.

2. Log into the Administration Console as MA (see [“Accessing the Administration Console” on page 2-21](#)) and follow the steps in the Bootstrap wizard to initialize the system.



Book: See section, "Bootstrapping the System" in Chapter 4 of the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information.

3. Create the required GA and UA accounts.

See [“Creating Administrators” on page 13-195](#) for more information.

4. As a GA, configure the required RiskFort rules to meet your business requirements.
See [Chapter 7, “Managing Global Rule Configurations”](#) for more information.
5. Enroll users with RiskFort.



Note: This step can be optional, if you configure your organization(s) for “[Implicit User Creation Mode](#)” on page 7-112. In this case, users are automatically enrolled during the first risk evaluation.

Use Java SDKs shipped with RiskFort for this purpose. See the Javadocs shipped with the SDKs2.2.6.

With this your system is set for risk evaluation. You can now manage the system ([Chapter 4, “Managing RiskFort Server Instances”](#)), administrators ([Chapter 13, “Managing Administrators”](#)), and users ([Chapter 14, “Managing Users”](#)).

For Complex Deployments

In larger enterprises, where the deployments are complex and high availability is a must, RiskFort can be implemented to provide adaptive authentication for the large user base, as well as administrators who manage the system. In these deployments, RiskFort components are installed on different servers. This is done for security, performance, high availability, and/or to enable multiple applications to use the adaptive-authentication capability.



Book: See Chapter 2, "Planning the Deployment" in the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information on this type of deployments.

[Table 1-4](#) summarizes the typical characteristics of this deployment type.

Table 1-4. Characteristics of Distributed Deployments

Characteristic	Details
Deployment Type	• Complex medium to large businesses • Enterprise deployments • Staging deployments
Geographic Expanse	Distributed across the globe
Deployment Requirements	• Ease of implementation and management • Global availability • High availability

The **quick overview** of the steps to set up and start managing strong authentication for your users is:

1. Ensure that RiskFort is installed and configured properly and that you have deployed the WAR files for the Administration Console and User Data Service.



Book: See Chapter 5, "Deploying RiskFort on a Distributed System" in the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information on installing RiskFort, deploying the WAR files, and performing other post-installation tasks in a distributed environment.

2. Log into the Administration Console as MA (see [“Accessing the Administration Console” on page 2-21](#)) and follow the steps in the Bootstrap wizard to initialize the system.



Book: See section, "Bootstrapping the System" in Chapter 4 of the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information.

3. Configure the Administration Console settings, which include UDS settings, global organization settings, Administration Console cache settings, and the basic username-password authentication policy for logging in to the console.
See [“Configuring Administration Console Settings” on page 2-25](#) for more information.
4. Set up RiskFort Server instances on different systems.
See [“Managing RiskFort Server Instances” on page 4-43](#) for more information.
5. Configure the protocols that Administration Console, SDKs, and Web Services use to communicate to RiskFort Server.
See [“Configuring Communication Protocols” on page 4-48](#) for more information.
6. Plan and create organizations. The organization architecture is flat and each organization that you create can map to a business unit in your enterprise.
See [“Creating and Activating Organizations” on page 10-148](#) for more information.
7. Plan and create the administrators (see [“Creating Administrators” on page 13-195](#)) and custom roles (see [Chapter 3, “Working with Custom Roles”](#)), if required.
8. Create appropriate rules and rulesets to meet your business requirements, and assign these configurations.

See [“Managing Global Rule Configurations” on page 7-73](#) for more information.

9. Enroll users with RiskFort.



Note: This step can be optional, if you configure your organization(s) for [Implicit User Creation Mode](#). In this case, users are automatically enrolled during the first risk evaluation.

Use Java SDKs shipped with RiskFort for this purpose. See the Javadocs shipped with the SDKs2.2.6.

10. If required, configure SSL-based communication between RiskFort Server and its clients.

See [“Creating Trust Stores” on page 4-47](#) for more information.

11. If you are planning to extend the RiskFort functionality by the use of Add-On rules or callouts, then define and configure the required configurations.

See [Chapter 12, “Working with Add-On Rules”](#) and [Chapter 9, “Configuring Callouts”](#) for more information.

With this your system is set for risk evaluation. You can now manage the system ([Chapter 4, “Managing RiskFort Server Instances”](#)), administrators ([Chapter 13, “Managing Administrators”](#)), and users ([Chapter 14, “Managing Users”](#)).

Chapter 2

Getting Started

This chapter walks you through the steps for logging in to the Administration Console as [Master Administrator](#) and configuring basic information, *after* you have successfully installed RiskFort and have deployed the console and bootstrapped it.



Book: See *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for detailed information on installing RiskFort, deploying the Administration Console, and bootstrapping it.

This chapter covers:

- [Accessing the Administration Console](#)
- [Changing Password and Profile Information](#)
- [Configuring Administration Console Settings](#)

Accessing the Administration Console

The default Master Administrator (MA) account is used to log into the Administration Console for the first time. Use the following out-of-the-box credentials to log in to the console:

- **User Name:** `masteradmin`
- **Password:** `master1234!`

To log in to the Administration Console:

1. Open a Web browser window.
2. Enter the URL to access Administration Console. The default Administration Console address is:

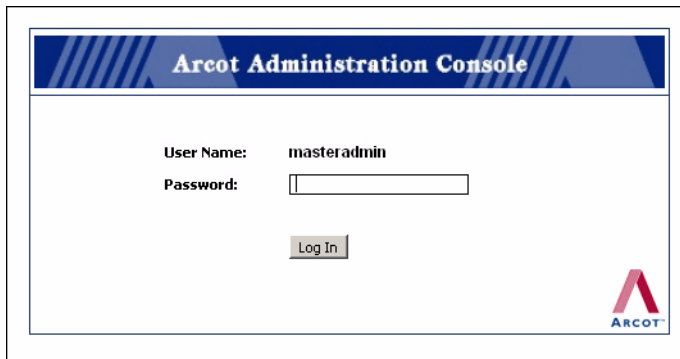
<http://<hostname>:<port>/arcotadmin/masteradminlogin.htm>

In the preceding URL:

- Replace *hostname* and *port* respectively with the host name or the IP address of the system where you have deployed the Administration Console and the port at which the console is listening.
- If you change the default application context (*arcotadmin*), then you must replace it with the new value.

The Master Administrator Login page appears, as shown in [Figure 2-1](#).

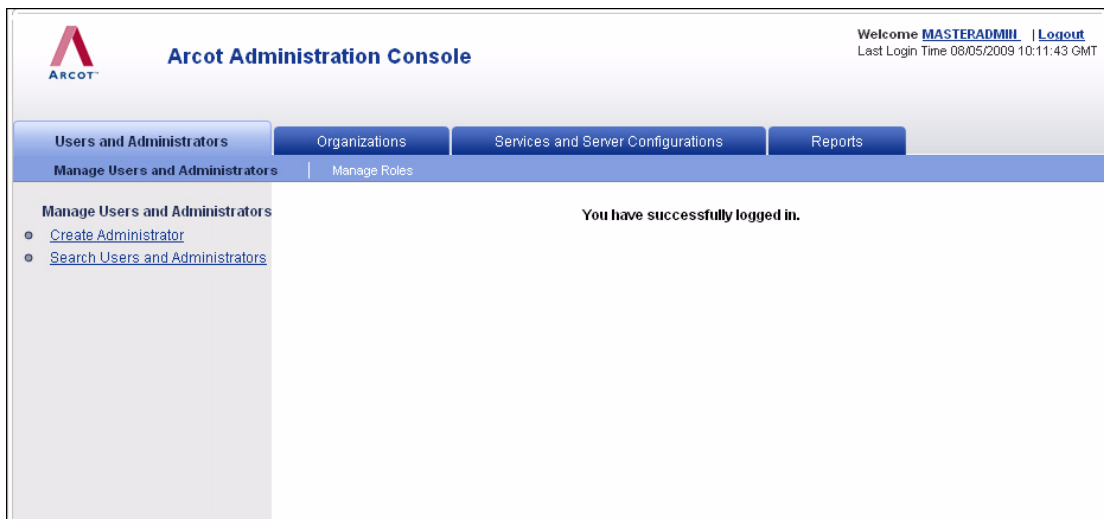
Figure 2-1 Master Administrator Login Page



3. Enter **master1234!** in the **Password** field and click **Log In**.

The landing page of the Administration Console appears, as shown in [Figure 2-2](#).

Figure 2-2 Master Administrator: Successfully Logged In



Security Recommendations While Using the Administration Console

To protect RiskFort from malicious attacks through the browser session, while using Administration Console, ensure that you:

- Do not share browser session with other applications.
- Do not open any other site while working with the Console.
- Enforce strict password restrictions for the Administration Console.
- Always log out after using the Administration Console.
- Close the browser window after the session is over.
- Assign proper roles to administrators according to the tasks they need to perform.

Logging Out of the Administration Console

To log out of the Administration Console, click the **Logout** link in the console Header area, which is located at the top-right corner.

Changing Password and Profile Information

Arcot strongly recommends that you change your Master Administrator password regularly to maintain high security, so that unauthorized persons do not gain access to the Administration Console using MA credentials.

Use the My Profile page, as shown in [Figure 2-3](#), to change your current password and your preferences that will be reflected by default for all administrator-related tasks that you perform in future.

Figure 2-3 Master Administrator: My Profile Page

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/15/2010 08:12:05 GMT

Users and Administrators | Organizations | Services and Server Configurations | Reports

My Profile

Update your personal details and preferences.

Change Password

Current Password:

New Password:

Confirm Password:

Administrator Preferences

Enable Preferred Organization: ☐

Preferred Organization:

Time Zone:

To change your current password and/or to set your organization preference:

1. Ensure that you are logged in as the MA.
2. Click the **MASTERADMIN** link in the console header.

The My Profile page, as shown in [Figure 2-3](#), appears.

3. In the **Change Password** section, specify:
 - a. The **Current Password**.
 - b. The **New Password**.
 - c. The new password again in the **Confirm Password** field.
4. In the **Administrator Preferences** section, specify:
 - a. Whether you would like to **Enable Preferred Organization** option.

This organization will be selected by default in the "Organization" field for all administrator-related tasks that you will perform from now on. For example, when you search the administrators, by default they will be searched in the preferred organization.

- b. The **Preferred Organization** that will be selected by default in the "Organization" field from now on.
- c. The preferred **Time Zone**.

This Time Zone will be shown from now on in the **Last Login** timestamp in the console Header. In addition, the reports data (such as Transaction Date) and Case-related dates and timestamps will use this Time Zone.

5. Click **Save**.

Configuring Administration Console Settings

Before you configure the RiskFort-specific settings, it is recommended that you configure the global configurations for the Administration Console, which include:

- User Data Service (UDS) configurations
- Organization global configurations
- Cache refresh configurations
- Basic authentication policy configurations

The following sub-sections walk you through the steps for configuring these global settings.

Updating UDS Configurations

User Data Service (UDS) is an Administration Console module for enabling access to the third-party data repositories (such as, LDAP directory servers) deployed by your organization. UDS enables RiskFort and the Administration Console to seamlessly access your existing data and leverage end-user information, without having to duplicate it in the standard Arcot SQL database tables.

Typically, you specify the UDS parameters while bootstrapping the system. However if you would like to update the UDS parameter settings, then use the User Data Service Configuration page ([Figure 2-4](#)) to do so.



Note: See section, "Bootstrapping the System" in *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information on setting UDS parameters.

Figure 2-4 User Data Service Configuration: Page 1

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 10/28/2009 09:40:02 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports

RiskFort | **Administration Console**

Administration Console

- **UDS Configuration**
 - [Organization Global Configuration](#)
 - [Cache Refresh Configuration](#)
- Authentication
 - [Basic Authentication Policy](#)

User Data Service Configuration

Configure the User Data Service (UDS) to access user information.
Note: It is optional to configure SSL between UDS and the Arcot Products.

User Data Service Configuration

Protocol :

Host :

Port :

Application Context Root :

Connection Timeout (in milliseconds) :

Read Timeout (in milliseconds) :

Idle Timeout (in milliseconds) :

Server Root Certificate :

Client Certificate :

Client Private Key :

Minimum Connections :

Maximum Connections :

To update the UDS configuration:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the tab's sub-menu.
4. If the User Data Service Configuration page is not already displayed, then click the **UDS Configuration** link to display the page (Figure 2-4.)

5. Specify the parameters explained in [Table 2-1](#) in the **User Data Service Configuration** section. All the parameters on this page are mandatory.

Table 2-1. UDS Configuration Parameters

Parameter	Default Value	Description
Protocol	TCP	The protocol to connect to the UDS service using the Administration Console. The available options are: • TCP • One-Way SSL • Two-Way SSL
Host	localhost	The IP address where the UDS service is available.
Port	8080	The port at which the UDS service is available.
Application Context Root	arcotuds	The unique base URL at which UDS is accessible in an application server instance (of the multiple Administration Console applications that are currently running.)
Connection Timeout (in milliseconds)	30000	Maximum time in milliseconds before the UDS service is considered unreachable.
Read Timeout (in milliseconds)	10000	The maximum time in milliseconds to wait for a response from UDS.
Idle Timeout (in milliseconds)	30000	The time (in milliseconds) after which an idle connection not serving requests will be closed.
Server Root Certificate		The path to the CA certificate file of UDS server. The file must be in PEM format.
Client Certificate		The path to the CA certificate file of the Administration Console. The file must be in PEM format.
Client Private Key		The location of file that contains the CA's private key. The path can be an absolute path or relative to <code>ARCOT_HOME</code> .
Minimum Connections	4	The minimum number of connections that will be created between the RiskFort Server and the UDS server.
Maximum Connections	32	The maximum number of connections that can be created between the RiskFort Server and the UDS server.

6. Click **Next** to continue with the configuration.

The next page, as shown in [Figure 2-5](#), appears.

Figure 2-5 User Data Service Configuration: Page 2

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/10/2010 10:23:18 GMT

Users and Administrators | Organizations | Services and Server Configurations | Reports

User Data Service Configuration

Configure the User Data Service (UDS) parameters to access user information.
Note: It is optional to configure SSL between UDS and the Arcot products.

Configure UDS Parameters

Search Configuration

Maximum Search Return Count:

LDAP Configuration

LDAP Connection Pool Initial Size:

LDAP Connection Pool Maximum Size:

LDAP Connection Pool Preferred Size:

LDAP Connection Pool Timeout (in milliseconds):

Authentication Token Configuration

Token Purge Interval (in seconds):

Authentication Token Validity Period (in seconds):

7. Specify the parameters explained in [Table 2-2](#) in the **User Data Service Configuration** section. All the parameters on this page are mandatory.

Table 2-2. UDS Search, LDAP, and Authentication Configuration Parameters

Parameter	Default Value	Description
Search Configuration		
Maximum Search Return Count	500	The maximum number of records that will be returned for all Search operations in the Administration Console.
LDAP Configuration		
LDAP Connection Pool Initial Size	2	The initial number of connections between UDS and LDAP that will be created in the pool.

Table 2-2. UDS Search, LDAP, and Authentication Configuration Parameters

Parameter	Default Value	Description
LDAP Connection Pool Maximum Size	5	The maximum number of connections allowed between UDS and LDAP.
LDAP Connection Pool Preferred Size	2	The preferred number of connections between UDS and LDAP.
LDAP Connection Pool Timeout (in milliseconds)	30000	The period for which UDS waits for a response from the LDAP, when a new connection is requested.
Authentication Token Configuration		
Token Purge Interval (in seconds)	3600	The maximum interval after which an authentication token is purged from the database, <i>after</i> the token expires.
Authentication Token Validity Period (in seconds)	86400	The maximum period (default is one day) after which an issued authentication token expires.

8. Click **Save** to save the changes you made.
9. Refresh *all* deployed RiskFort Server instances. See [“Refreshing or Shutting Down a Server Instance”](#) on page 4-52 for instructions on how to do this.

Specifying Global Settings for Organizations

When you deploy the Administration Console, an organization is created by default along with the MA account. This out-of-the-box organization is referred to as *Default Organization* (DEFAULTORG).

As a single-organization system, the Default Organization is useful because you do not need to create any new organizations. You can configure the Default Organization settings, change its Display Name, and then continue to use it for administering purposes. In the case of a multi-organization system, however, you can either rename the Display Name of the Default Organization, configure its settings, and continue to use it as the default, or you can create a new organization and set it as the Default Organization.



Note: Typically when you create administrators or enroll users *without* specifying their organization, then they are created in the Default Organization.

The Organization Global Configuration page (Figure 2-6) enables you to select the organization that will be used as the Default Organization and to control whether all future organizations in the system will inherit the settings of the Default Organization or can be edited individually to override these settings.

Figure 2-6 Organization Global Configuration Page



To specify the Default Organization and whether configurations can be set at the organization-level:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the tab's sub-menu.
4. In the tasks pane, click the **Organization Global Configuration** link to display the corresponding page (Figure 2-6.)
5. Under **Organization Configuration**, deselect the **Allow Configuration at Organization Level** option, if you do not want to set organization-specific configurations.
By default, this option is enabled.
6. Under **Default Organization**, select the organization that you want to set as the Default Organization from the **Organization Name** list.

- Click **Save** to save the changes you made on this page.

Specifying Cache Refresh Settings

Administration Console caches certain data, which serves frequently-accessed console pages and UDS data faster. Typically organizations and roles are cached. The configuration for this can be updated by using the Cache Refresh Configuration page (Figure 2-7.)

Figure 2-7 Cache Refresh Configuration Page

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo and 'Arcot Administration Console' title are visible. The top navigation bar includes tabs for 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (which is active), and 'Reports'. Below this, a sub-menu for 'Administration Console' is shown, with 'Cache Refresh Configuration' selected. The main content area is titled 'Cache Refresh Configuration' and includes a subtitle: 'Update the cache settings for User Data Service and the Administration Console.' There are two configuration sections: 'User Data Service' and 'Administration Console'. Each section contains a checkbox for 'Enable Automatic Refresh' (both are checked) and a text input for 'Refresh Interval (in minutes)' (both are set to '30'). Each section also has 'Save' and 'Refresh Now' buttons.

To update the UDS and/or Administration Console cache settings:

- Ensure that you are logged in as the MA.
- Activate the **Services and Server Configurations** tab.
- Click the **Administration Console** option on the tab's sub-menu.
- In the tasks pane, click the **Cache Refresh Configuration** link to display the corresponding page (Figure 2-7.)
- In the **User Data Service** and/or **Administration Console** sections:
 - Deselect or select the **Enable Automatic Refresh** option, as required.

- b. Edit the **Refresh Interval** value.

The cache will be refreshed at the interval that you specify. For example, if you enter **60**, then it is automatically refreshed every hour. The default value is 30 minutes.

- c. Click **Save** to save the changes.
- d. If you want to refresh the changes immediately, then click **Refresh Now**.

Specifying Basic Authentication Policy Settings

Administrators logging into the Administration Console can be authenticated either by using the Basic Authentication Policy or WebFort User-Password mechanism. The mechanism that will be used is determined by the option that you selected while creating the organization:

- If you selected the **Basic** option while creating an organization, then you can use the default authentication policy, as discussed in the “[Specifying the Basic Authentication Password Policy](#)” section (for global level).
- If you selected the **WebFort User Password** option, then ensure that Arcot WebFort 6.0 is deployed and accessible.



Book: See *Arcot WebFort 6.0 Installation and Deployment Guide* and *Arcot WebFort 6.0 Administration Guide* for detailed information to install and configure WebFort in your environment.

Specifying the Basic Authentication Password Policy

As the name implies, *Basic Authentication* method involves administrators to log into the console by using a user ID and the corresponding password.

You can use the Basic Authentication Policy page ([Figure 2-8](#)) to strengthen the password policy by enforcing restrictions, such as password length, allowed number of special characters, and the number of failed login attempts allowed before locking the account.

Figure 2-8 Basic Authentication Policy Page



Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 01/07/2010 09:18:41 GMT

Arcot Administration Console

Users and Administrators

Organizations

Services and Server Configurations

Reports

RiskFort

Administration Console

Administration Console

- [UDS Configuration](#)
- [Organization Global Configuration](#)
- [Cache Refresh Configuration](#)

Authentication

- Basic Authentication Policy**

Basic Authentication Policy

Specify the Basic Authentication password policy.

Password Policy Configuration

Minimum Password Length: *	6 Enter a value between 6 and 32.
Maximum Password Length: *	25 Enter a value between 6 and 32.
Maximum Failed Attempts: *	5 Enter a value between 3 and 10.
Minimum Numeric Characters: *	1 Enter a value between 0 and 32.
Minimum Alphabetic Characters: *	4 Enter a value between 0 and 32.
Minimum Special Characters: *	1 Enter a value between 0 and 32.
Allowed Special Characters:	!@#\$\$%^&*()_+
Validity Period: *	☒ 180 days ☐ Never Expires

Save

To specify the Basic Authentication policy:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the tab's sub-menu.
4. In the tasks pane, click the **Basic Authentication Policy** link to display the corresponding page (Figure 2-8.)
5. Specify the parameters explained in Table 2-3 in the **Password Policy Configuration** section. All the parameters on this page are mandatory.

Table 2-3. Basic Authentication Policy Parameters

Parameter	Default Value	Description
Minimum Password Length	6	The least number of characters that the password must contain. You can set a value between 6 and 32 characters.
Maximum Password Length	25	The most number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of Allowed Special Characters that the password must contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#\$%^&*()_+ +	The list of special characters that the password can contain.
Validity Period	180 days	The maximum number of days for which a password is valid.

- Click **Save** to save the changes you made on this page.

Chapter 3

Working with Custom Roles



Important: The role management tasks discussed in this chapter can *only* be performed by the **Master Administrator**.

RiskFort is shipped with out-of-box roles that are associated with pre-defined privileges. (See [“Supported Roles” in Chapter 1](#) for more information on this topic.) However, RiskFort also provides you the capability to manipulate these pre-defined roles in case:

- The default roles do not meet your organization’s requirements.
- You need to manage a role information that is different from the one provided by RiskFort.

This chapter explores the ability to create and apply custom roles in RiskFort, which are a major benefit. This chapter guides you through:

- [Understanding Custom Roles](#)
- [Creating a Custom Role](#)
- [Updating a Custom Role Information](#)
- [Deleting a Custom Role](#)

Understanding Custom Roles

As an MA, you can create *new administrative roles* that inherit a subset of privileges from one of the following pre-defined parent roles (as discussed in [Chapter 1, “Overview of the Administration Console”](#)):

- [Global Administrator](#)
- [Organization Administrator](#)
- [User Administrator](#)

These roles are called *custom roles*, and are derived by **disabling** some of the default privileges associated with the parent role. For example if you need to disable the "Organization Creation Privilege" for a GA, then you can create a custom role by disabling this privilege.

When you create a custom role, it becomes available as a role option when you create or update an administrative account. In addition to creating custom roles, you can also update and delete them. See the following sections in this chapter for more information on management of custom roles.

Things That You Should Know About Custom Roles

- *Only* an MA can create custom roles.
- A custom role can only inherit the subset of privileges from a single role. In other words, a custom role *cannot* inherit privileges from two different roles.

For example, you *cannot* create a custom UA role that has privileges to manage users (UA privilege) and create organizations (OA privilege.)

- You cannot assign new privileges to a custom role, if the parent role does not have these privileges.

For example, if the pre-defined OA roles does not have the privilege to Create an Organization, then the custom role based on this OA role cannot have that privilege either.

- When you create a custom role, a task representing one or more privileges will continue to be visible, as long as at least one of the privileges is *still* available.

For example, the "Search Organizations" link will appear if the Update privilege is still available, even though the Activate, Deactivate, and Delete privileges are disabled.

- A new custom role is available to other instances of Administration Console *only after* you refresh the Administration Console server cache.

Pre-Defined Custom Roles

In addition to the custom roles that you can create, RiskFort is also shipped with three pre-defined custom roles (as shown in [Figure 1-4](#) in [Chapter 1, "Overview of the Administration Console"](#)) that are required for Case Management. These roles include:

- **QM:** The **Queue Manager** role is shipped with the required privileges to supervise cases. This role is derived from the default [Organization Administrator](#) role.
- **CSR:** The **Customer Support Representative** role is shipped with the required privileges to work on cases and handle end-user calls. This role is derived from the default [User Administrator](#) role.

- **FA:** The **Fraud Analyst** role is shipped with the required privileges to analyze cases to find hidden trends and patterns. This role is also derived from the default [User Administrator](#) role.



Note: See [Chapter 15, “Managing Cases”](#) for detailed information on Case Management and the Queue Manager, Customer Support Representative, and Fraud Analyst roles.

You can see these out-of-the-box custom roles on the Update Custom Role page ([Figure 3-2 on page 3-40.](#))

Creating a Custom Role

To create a custom role:

1. Ensure that you are logged in as the MA.
2. Activate the **Users and Administrators** tab.
3. Under **Manage Roles**, click the **Create Custom Role** link. The Create Custom Role page ([Figure 3-1](#)) appears.

Figure 3-1 Create Custom Role Page

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/15/2010 08:12:05 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports**

Manage Users and Administrators | **Manage Roles**

Manage Roles

- **Create Custom Role**
- [Update Custom Role](#)
- [Delete Custom Role](#)

Create Custom Role

Create a custom administrator role. This role must be derived from one of the predefined roles and can have a subset of the base role's privileges.

Role Details

Role Name:

Role Display Name:

Role Description:

Role Based On:

Set Privileges

Available Privileges

- Update Administrator
- RiskFort - Evaluate Risk
- View Advice Summary Report
- RiskFort - Get User Details
- View User Activity Report
- RiskFort - Post Evaluate
- View Exception User Report
- View Administrator Activity Report
- Deactivate User
- Delete User

Unavailable Privileges

4. In the **Role Details** section, specify the following information:
 - **Role Name:** The unique name to identify the new role. This name is used internally by RiskFort by authenticating and authorizing this new role.
 - **Role Display Name:** The descriptive name of the role that appears on all other Administration Console pages and reports.
 - **Role Description:** The useful information related to the role for later reference.
 - **Role Based On:** The pre-existing role from which this custom role should be derived.
5. In the **Set Privileges** section, specify the roles that will *not* be available to the new role:
 - a. In the **Available Privileges** list, select all the privileges that you need to *disable* for the custom role.

This list displays all the privileges available to the administrative role that you selected in the **Role Based On** field.



Note: You can hold the **Ctrl** key to select more than one privileges at a time.

- b. Click the > button to move the selected privileges to the **Unavailable Privileges** list.
6. Click **Create** to create the custom role.

Updating a Custom Role Information

To update an existing custom role definition:

1. Ensure that you are logged in as the MA.
2. Activate the **Users and Administrators** tab.
3. In the tasks menu under the **Manage Roles** section, click the **Update Custom Role** link.

The Update Custom Role page, as shown in [Figure 3-2](#), appears.

Figure 3-2 Update Custom Role Page

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo, the title 'Arcot Administration Console', and a user status bar indicating 'Welcome MASTERADMIN | Logout' and 'Last Login Time 06/15/2010 08:12:05 GMT'. Below the header is a navigation bar with tabs for 'Users and Administrators', 'Organizations', 'Services and Server Configurations', and 'Reports'. The 'Users and Administrators' tab is active, showing a sub-menu with 'Manage Users and Administrators' and 'Manage Roles'. The 'Manage Roles' sub-menu is selected, displaying a list of actions: 'Create Custom Role', 'Update Custom Role' (highlighted with a green dot), and 'Delete Custom Role'. The main content area is titled 'Update Custom Role' and includes a subtitle 'Update a custom role.' Below this, there are two main sections: 'Role Details' and 'Set Privileges'. The 'Role Details' section contains four fields: 'Role Name' (a dropdown menu showing '--Select--'), 'Role Display Name' (a text input field), 'Role Description' (a text input field), and 'Role Based On' (a text input field). The 'Set Privileges' section contains two lists: 'Available Privileges' and 'Unavailable Privileges', each with a list box and a vertical scrollbar. Between these lists are four buttons: '>', '>>', '<', and '<<'. At the bottom of the page, there is an 'Update' button.

4. Select the **Role Name** that you want to update.
5. Make the required changes to one or all of the fields in the **Role Details** section.
6. In the **Set Privileges** section, if required, specify the list of privileges that will *not* be available to the role:
 - a. In the **Available Privileges** list, select all the privileges that you need to *disable* for the new role.

This list displays all the privileges available to the administrative role that you selected in the **Role Based On** field.

or
 - b. In the **Unavailable Privileges** list, select the privileges that you want to *enable* for the new role.

This list displays all the privileges that are not available to the administrative role that you selected in the **Role Based On** field.



Note: You can hold the **Ctrl** key to select more than one privileges at a time.

- c. Click the > button to move the selected privileges to the **Unavailable Privileges** list.
7. Click **Update** to update the Custom role definition.

Deleting a Custom Role



Important: You *cannot* delete a custom role that is currently assigned to an administrator.

If you need to delete such a role, then you must first change the role of all administrators who have been assigned this role by using the Update Administrator page ([Figure 13-8](#)) and then follow the instructions in this section.

To delete an existing custom role:

1. Ensure that you are logged in as the MA.
2. Activate the **Users and Administrators** tab.
3. In the tasks menu under the **Manage Roles** section, click the **Delete Custom Role** link.

The Delete Custom Role page, as shown in [Figure 3-3](#), appears.

Figure 3-3 Delete Custom Role Page

The screenshot shows the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title 'Arcot Administration Console' is in the center. On the right, a user is logged in as 'MASTERADMIN' with a 'Logout' link and a 'Last Login Time' of '01/07/2010 09:18:41 GMT'. Below the header, there are four main navigation tabs: 'Users and Administrators', 'Organizations', 'Services and Server Configurations', and 'Reports'. The 'Users and Administrators' tab is active, and within it, the 'Manage Roles' sub-tab is selected. On the left side of the 'Manage Roles' section, there are three links: 'Create Custom Role', 'Update Custom Role', and 'Delete Custom Role', with the last one being highlighted with a green dot. The main content area is titled 'Delete Custom Role' and includes a warning message: 'Delete a custom role. A role can be deleted only if no administrators have currently been assigned that role.' Below this is a 'Role Details' form with four fields: 'Role Name' (a dropdown menu currently showing '--Select--'), 'Role Display Name' (a text input field), 'Role Description' (a text input field), and 'Role Based On' (a text input field). A 'Delete' button is located at the bottom of the form.

4. In the **Role Details** section, select the custom role that you need to delete from the **Role Name** list.
5. Click **Delete** to delete the selected custom role.

Chapter 4

Managing RiskFort Server Instances



Important: All the configurations and tasks discussed in this chapter can *only* be performed by **Master Administrator**.

As a Master Administrator, you will need to manage a RiskFort instance locally. However, before you can manage a server instance, you must configure the connectivity parameters to connect to the instance. (See section, [“Configuring Server Connectivity”](#), for information on how to do this.)

Only after you have configured the connectivity parameters, can you manage the RiskFort Server instance. The tasks for managing an instance include:

- [Configuring Server Connectivity](#)
- [Creating Trust Stores](#)
- [Configuring Communication Protocols](#)
- [Refreshing or Shutting Down a Server Instance](#)



Note: The last task (Refreshing or Shutting Down a Server Instance) can also be performed by using system tools, as discussed in [Chapter 17, “Tools for System Administrators”](#).

Configuring Server Connectivity

RiskFort comprises two server components:

- **RiskFort Server**, which is the core engine for risk evaluations.
- **Case Management Queuing Server**, which is the core engine for Case Management and is responsible for building and prioritizing cases according to the Queue definition.



Note: At any time, all instances of Administration Console can only connect to a single instance of the Case Management Queuing Server.

You must use the RiskFort Connectivity page ([Figure 4-1](#)) to configure the connection settings that will be used by the Administration Console to connect to your RiskFort Server and the Case Management Queuing Server instance.

Figure 4-1 RiskFort Connectivity Page

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 07/06/2010 16:15:06 GMT

Navigation: Users and Administrators | Organizations | **Services and Server Configurations** | Reports

RiskFort | Administration Console

RiskFort Connectivity

Specify the configurations that will be used by the Administration Console to connect to the RiskFort Server instance.

Server:
 Port:
 Transport:
 Server CA Root Certificate: [Browse...](#)
 Client Certificate-Key Pair in PKCS#12: [Browse...](#)
 Client PKCS#12 Password:

[Save](#)

Case Management Queuing Server Connectivity

Specify the configurations that will be used by the Administration Console to connect to the Case Management Queuing Server instance.

Host:
 Backup Host:
 Port:
 Transport:
 Server CA Root Certificate: [Browse...](#)
 Client Certificate-Key Pair in PKCS#12: [Browse...](#)
 Client PKCS#12 Password:

[Save](#)

System Configuration

- RiskFort Connectivity**
 - [Trusted Certificate Authorities](#)
 - [Protocol Configuration](#)

Extensible Configurations

- [Add Rule Type](#)
- [View Existing Rule Types](#)

To specify the connectivity parameters for the two server modules:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. If not already displayed, click the **RiskFort Connectivity** link in the tasks pane to display the corresponding page (Figure 4-1.)
4. Use the information in Table 4-1 to edit the fields in the **RiskFort Connectivity** section.

Table 4-1. Connection Parameters Between RiskFort Server and the Administration Console

Field	Description
Server	Enter the IP address of the system where you installed the required RiskFort Server instance. Note: Ensure that the system where RiskFort Server is installed must be accessible by its hostname on the network.
Port	Enter the port on which service for the protocol is exposed.
Transport	Specify the transport mode (TCP or SSL) for the corresponding component (Server Management Web Services, Administration Web Services, Transaction Web Services, and Authentication Native) to connect to the specified RiskFort Server instance.
Server CA Root Certificate	Browse to and upload the server CA root certificate. Note: This server certificate must be in PEM format.
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store that contains the client certificate and the private key.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

5. Use the information in Table 4-2 to edit the fields in the **Case Management Queuing Server Connectivity** section.

Table 4-2. Connection Parameters Between Case Management Queuing Server and the Administration Console

Field	Description
Host	Enter the IP address of the system where you installed the Queuing Server instance. Note: Ensure that the system where Queuing Server is installed must be accessible by its hostname on the network.
Backup Host	If installed, enter the IP address of the system where the backup Queuing Server instance is available. Note: Ensure that the system where Queuing Server is installed must be accessible by its hostname on the network.
Port	Enter the port on which service for the protocol is exposed.
Transport	Specify the transport mode (TCP or SSL) for the corresponding component (Server Management Web Services, Administration Web Services, Transaction Web Services, and Authentication Native) to connect to the specified RiskFort Server instance.
Queueing Server CA Root Certificate	Browse to and upload the server CA root certificate. Note: This server certificate must be in PEM format.
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store that contains the client certificate and the private key.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

- Click **Save** to save the configurations that you have set and to ensure that the Administration Console gets the details of the instance.

Creating Trust Stores

You can create a trust store to authenticate RiskFort components (that include Administration Console and Java SDKs) or other clients to a RiskFort server instance during SSL-based communications. A *trust store* contains a set of CA root certificates trusted by RiskFort Server instances and the Case Management Queuing Server.

You can use the Trusted Certificate Authorities page (Figure 4-2) to create trust stores and to add new root certificates to your trust stores.

Figure 4-2 Trusted Certificate Authorities Page

The screenshot shows the Arcot Administration Console interface. The top navigation bar includes 'Users and Administrators', 'Organizations', 'Services and Server Configurations', and 'Reports'. The 'Services and Server Configurations' tab is active, and the 'RiskFort' sub-tab is selected. The left sidebar shows a tree view under 'RiskFort' with 'System Configuration' expanded, highlighting 'Trusted Certificate Authorities'. The main content area is titled 'Trusted Certificate Authorities' and contains the instruction: 'Upload multiple CAs and group them to create an SSL Trust Store.' Below this is a form with the following fields and buttons:

- Name :** A text input field.
- Root CAs :** Two text input fields, each followed by a 'Browse...' button.
- Add More** button.
- Save** button at the bottom right.

To create a trust store for your RiskFort Server instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **RiskFort** tab in the sub menu is active.
3. Under the **System Configuration** section, click the **Trusted Certificate Authorities** link to display the Trusted Certificate Authorities page (Figure 4-2.)
4. Enter the name for the new trust store that you want to create in the **Name** field.
5. Click the corresponding **Browse** buttons to upload one or more root certificates of the trusted CAs. You can click **Add More** to display additional fields for uploading certificates.

- Click **Save** when you finish uploading all required certificates.

Configuring Communication Protocols

The Protocol Configuration page is divided in two sections: **RiskFort Protocol Configuration** section and the **Case Management Queuing Server Protocol Configuration** section.

By using the **RiskFort Protocol Configuration** section (Figure 4-3), you can configure the protocols that Administration Console, SDKs, and Web Services use to communicate with your RiskFort Server instance for authentication and administration purposes. In addition to the port on which the server listens to each of these enabled components, you can also specify the transport security mechanism (TCP or SSL.) In case you specify this mechanism as SSL, then you must also specify the valid and trusted client component's certificate and private key that are required for establishing a secure connection.

Figure 4-3 The RiskFort Protocol Configuration Section

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 07/06/2010 16:15:06 GMT

Services and Server Configurations

RiskFort Protocol Configuration

Configure the protocols for the RiskFort Server instance. If you are using SSL security, both the Certificate Chain and the Private Key must be uploaded in PEM format. The changes made using this screen are not effective until the RiskFort Server is restarted.

Enabled	Protocol	Port Number	Transport Security	Client Store	SSL Certificate Details
☒	Native (TCP)	7680	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☒	Server Management	7980	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☒	Administration Web Service	7777	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☒	Transaction Web Service	7778	TCP	--Select--	Certificate Chain : Browse... Private Key : Browse...
☐	Native (SSL)	7681	SSL	--Select--	Certificate Chain : Browse... Private Key : Browse...

[Save](#)

[Table 4-3](#) explains the protocols that you see in the **RiskFort Protocol Configuration** section on the page and lists their default port numbers.

Table 4-3. RiskFort Protocols and Port Numbers

Protocol	Default Port Number	Description
Native (TCP)	7680	This is an Arcot proprietary protocol to enable communication between the RiskFort Server instance and the RiskFort Java SDKs (which include Risk Evaluation and Issuance.)
Server Management	7980	The arrfadmin tool communicates with the RiskFort Server instance for server management activities (graceful shutdown and server cache refresh) by using this protocol. See “arrfadmin: Server Refresh and Shutdown Tool” on page 17-302 for detailed information on this Administration Console tool.
Administration Web Service	7777	This is the protocol for communication between RiskFort Server and Administration Web services. The RiskFort Server listens to the Administration Web service calls on this port. Note: These calls do <i>not</i> include the RiskFort Issuance or Risk Evaluation calls.
Transaction Web Service	7778	This protocol is used by the Risk Evaluation and the Issuance Web services to connect to the RiskFort Server instance. Note: These calls do <i>not</i> include the Administration service calls.
Native (SSL)	7681	This is an Arcot proprietary protocol to enable SSL-based communication between the RiskFort Server instance and the RiskFort Java SDKs (which include Risk Evaluation and Issuance.)

Similarly, by using the **Case Management Queuing Server Protocol Configuration** section ([Figure 4-4](#)), you can configure the protocols that Administration Console and the Case Management Queuing Server use to communicate with your RiskFort Server instance for authentication and administration purposes. In addition to the port on which the server listens to each of these enabled components, you can also specify the transport security mechanism (TCP or

SSL.) In case you specify this mechanism as SSL, then you must also specify the valid and trusted client component's certificate and private key that are required for establishing a secure connection.

Figure 4-4 The Case Management Queuing Server Protocol Configuration Section

Case Management Queuing Server Protocol Configuration

Configure the protocols for the Case Management Queuing Server instance. If you are using SSL security, both the Certificate Chain and the Private Key must be uploaded in PEM format. The changes made using this screen are not effective until the Case Management Queuing Server is restarted.

Enabled	Protocol	Port Number	Transport Security	Client Store	SSL Certificate Details
☒	Case Management Queuing Server	7779	TCP	--Select--	Certificate Chain : Browse Private Key : Browse
☒	Case Management Queuing Administration	7780	TCP	--Select--	Certificate Chain : Browse Private Key : Browse

Table 4-4 explains the protocols that you see in the **Case Management Queuing Server Protocol Configuration** section on the page and lists their default port numbers.

Table 4-4. Case Management Queuing Server Protocols and Port Numbers

Protocol	Default Port Number	Description
Queueing Server	7779	This protocol is used by the Queueing Server module to listen to the Case Management requests (at the server end) on the specified port.
Queueing Administration	7780	This is the protocol for communication between RiskFort Server and Queueing Management. The RiskFort Server listens to the Case Management Web service calls on this port.

To configure RiskFort Server and the Case Management Queuing Server network protocols:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.

3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **System Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page (Figure 4-3.)
5. Edit the fields on the page, as required. Table 4-5 explains these fields.

Table 4-5. RiskFort and Case Management Queuing Server Setup Page Fields

Page Column	Action Description
Protocol	Use the check box in the Enabled column, to enable the required protocols. See Table 4-3 for more information on the supported protocols.
Port Number	Enter the port number where the corresponding RiskFort service is available. The following are the default port numbers for RiskFort protocols: • RiskFort Native (TCP): 7680 • RiskFort Native (SSL): 7681 • Administration Web Services: 7777 • Transaction Web Services: 7778 • Queuing Server: 7779 • Queueing Administration: 7780 • Server Management: 7980
Transport Security	Specify one of the following modes that are supported for data transfer: • TCP: Transmission Control Protocol (TCP) mode is the default mode that is supported by both RiskFort protocols. It sends data in the clear. • SSL: Secure Sockets Layer (SSL) provides higher security for transactions, because it encrypts and decrypts data that is being transmitted.
Client Store	Select the trust store that contains the root certificates of the trusted CAs. See section “ Creating Trust Stores ” for more information on configuring trust stores.
SSL Certificate Details	Specify the certificate chain that is used by the SSL transport security mode. Upload the Certificate Chain and Private Key of the certificate using the respective Browse buttons in the corresponding fields. Important: Ensure that the certificates in the chain that you upload here must follow the Leaf certificate --> Intermediate CA certificates --> Root certificate hierarchy. The certificate and the key <i>must</i> be in PEM format.

6. Click **Save** after you complete the configurations on the page.
7. Refresh the RiskFort Server instance for which you made the preceding changes. See “[Restarting a Server Instance](#)” for instructions on how to do this.

Configuring SSL Communication (Optional)

By default, Administration Console uses Transmission Control Protocol (TCP) to communicate with RiskFort Server. However, TCP is vulnerable to spoofing and man-in-the-middle attacks. By using the Administration Console, you can configure SSL to ensure secure communication between:

- Administration Console and RiskFort Server
- RiskFort Server and Java SDKs
- RiskFort Server and [arrfadmin](#) Tool
- [arrfadmin](#) tool and Case Management Queuing Server



Book: See Appendix F, "Configuring SSL" in the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for step-by-step configuration of SSL-based communication between these components.

See "[arrfadmin: Server Refresh and Shutdown Tool](#)" in [Chapter 17](#) for more information on the [arrfadmin](#) tool.

Refreshing or Shutting Down a Server Instance

This section covers:

- [Refreshing a Server Instance](#)
- [Restarting a Server Instance](#)

Refreshing a Server Instance

You can use the [arrfadmin](#) tool to refresh both, RiskFort Server and the Case Management Queuing Server instances.



Important: Before you run the `arrfadmin` tool for RiskFort Server as directed in the following sub-sections, set the `Host` and `Port` values in `riskfortadminclient.ini`. See “Configuring the Tool for Two-Way SSL Communication with the Server” on page 17-305 for more information.

See “arrfadmin: Server Refresh and Shutdown Tool” on page 17-302 for more information on the tool.

On Windows

Run the `arrfadmin` tool to refresh the RiskFort Server cache as follows:

1. Open the Command Prompt window.
2. Navigate to the following directory:


```
<install_location>\Arcot Systems\bin\
```
3. To refresh:
 - **RiskFort Server instance:**

```
arrfadmin -r
```
 - **Case Management Queuing Server instance:**

```
arrfadmin <host_name> <port> -r
```

On UNIX-Based Platforms

Run the `arrfadmin` tool to refresh the RiskFort Server cache as follows:

1. Open the terminal window.
2. Navigate to the following directory:


```
<install_location>/arcot/bin/
```
3. To refresh:
 - **RiskFort Server instance:**

```
arrfadmin -r
```
 - **Case Management Queuing Server instance:**

```
arrfadmin <host_name> <port> -r
```

Restarting a Server Instance

The following sub-sections walk you through the steps for restarting the RiskFort Server and the Case Management Queuing Server instance.

On Windows

To start a server instance on Windows:

1. Log in to the computer where the instance has stopped.
2. Click the **Start** button on the desktop.
3. Navigate to **Settings, Control Panel, Administrative Tools, and Services**.
4. To restart:
 - **RiskFort Server instance:** Double-click **Arcot RiskFort Service** from the listed services.
 - **Case Management Queuing Server:** Double-click **Arcot RiskFort Case Management Queuing Service** from the listed services.
5. Click **Start** to start the service.

On UNIX-Based Platforms

To start a server instance on UNIX-based platforms:

1. Log in to the computer where the instance must be started.
2. Navigate to the following directory:
`<install_location>/arcot/bin/`
3. Run the following command to restart:

- **RiskFort Server instance:**
`./riskfortserver start`
- **Case Management Queuing Server instance:**
`./casemanagementserver start`

Chapter 5

Understanding RiskFort Rule Basics



Important: Most of the tasks related to the concepts discussed in this chapter can *only* be performed by **Global Administrators and Organization Administrators**. However, this chapter is useful for anyone who wants to understand the basics of rules used by RiskFort.

RiskFort uses various rules to evaluate the risk associated with each transaction. These rules can be broadly categorized in to the following two categories:

- [Evaluation Rules](#)
- [Scoring Engine](#)

Irrespective of the category the rule belongs to, every rule in RiskFort has three specific characteristics that govern how the rule is processed:

- Ruleset
- Rule Implementation (at global or organization level)
- Rule Type

A rule and Ruleset type are closely related. Each rule *must* belong to a **Ruleset**. This choice of the Ruleset determines the options that are available for a rule. Similarly, the **Rule Implementation** determines whether the rule is applicable at the global level (available as a template to organizations) or at the level of individual organizations. **Rule Type** determines the capability and scope of the rule, and is closely associated with [Add-On Rules](#).



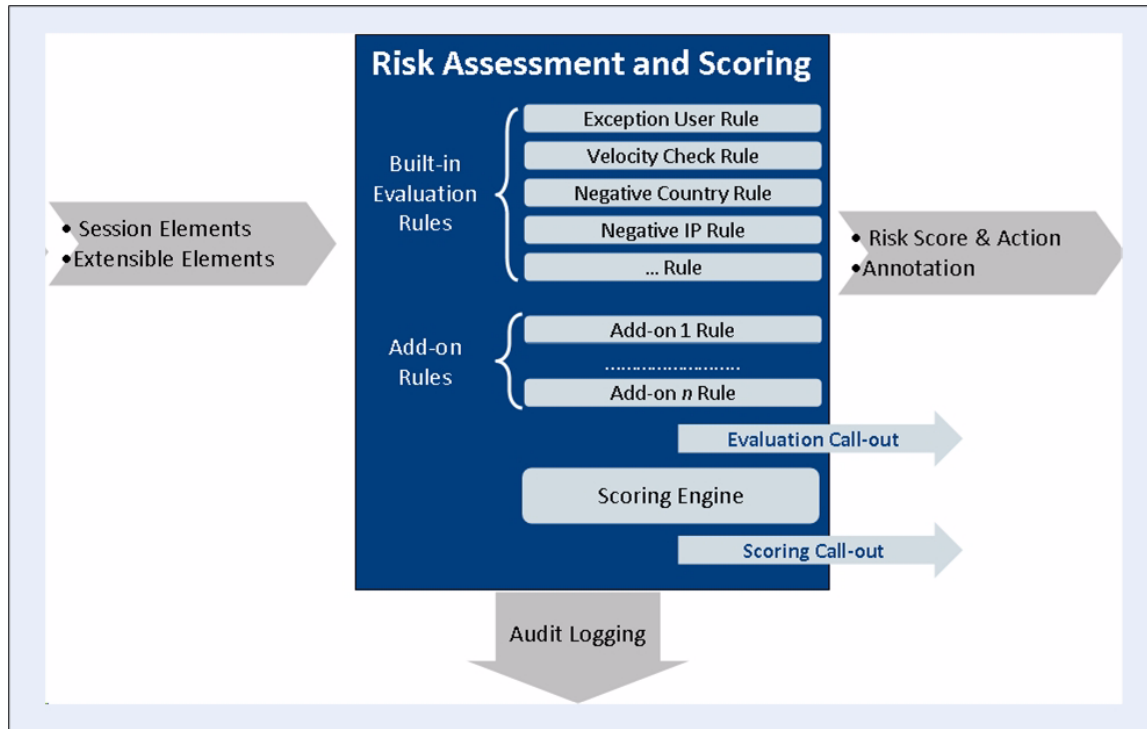
Note: See [“Creating Rulesets” in Chapter 7](#) for information on working with Rulesets.

See [Chapter 7, “Managing Global Rule Configurations”](#) and [Chapter 11, “Managing Organization-Specific RiskFort Configurations”](#) for implementing rules at global and organization level, respectively.

See [Chapter 6, “Preparing for Add-On Rules: Working with Rule Types”](#) for information on managing Rule Types in RiskFort.

Figure 5-1 is a schematic diagram of RiskFort rules and their scoring order, with respect to various rules. The subtypes of all Evaluation and Scoring rules shown in Figure 5-1 are discussed in subsections that follow the figure.

Figure 5-1 RiskFort Rules and Scoring Order



Evaluation Rules

Each *Evaluation rule* is a pre-configured logic that returns a boolean value. For a risk evaluation request from your application, this logic is applied to the incoming transaction data in the request. If the rule-logic matches, then each rule returns **TRUE**, if the rule matched; and **FALSE**, if it did not.



Important: During scoring, Evaluation rules are scored in the order of priority until a match is detected.

RiskFort provides the following types of Evaluation rules:

- [Out-Of-Box Rules](#)
- [Add-On Rules](#)
- [Evaluation Callout](#)

Out-Of-Box Rules

These are *terminating rules*. In other words, if during scoring any Evaluation rule matches (returns [True](#)), then the Risk Engine stops scoring the following rules in this category and generates a Risk Score corresponding to the matched rule.

These rules, in turn, can be categorized as:

- [Configurable Built-In Rules](#)
- [Non-Configurable Built-In Rules](#)

Configurable Built-In Rules

[Table 5-1](#) lists the out-of-the-box rules that are installed and deployed by default when you install RiskFort.

Table 5-1. Configurable Built-In Rules

Rule Name	Rule Description
Exception User Check	An organization may choose to temporarily exclude a user from risk evaluation for a specified time interval. For example, a user might need to travel to a Negative Country. Such users are added to the <i>Exception User List</i>, and are referred to as <i>exception users</i>. If found in the Exception User List, by default RiskFort returns a low Score and the ALLOW advice for transactions originating from exception users.
Unknown User Check	The user does not exist in the RiskFort database. In such cases, RiskFort returns ALERT. Your application can either call the RiskFort API to create the user in RiskFort, or take an appropriate action.
Trusted IP/Aggregator Check	See “Configuring Trusted IP Addresses” and “Configuring Trusted Aggregators” for more information.
Negative IP Check	See “Configuring Negative IP Addresses” for more information.
Negative Country Check	See “Configuring Negative Country List” for more information.

Table 5-1. Configurable Built-In Rules

Rule Name	Rule Description
User Velocity	See “Configuring User Velocity” for more information.
Device Velocity	See “Configuring Device Velocity” for more information.
Zone Hopping	See “Configuring Zone Hopping” for more information.

Non-Configurable Built-In Rules

In addition to the preceding configurable rules, RiskFort also verifies:

- *If* a user (whose transaction is being evaluated) exists in the RiskFort database. This information is used for Machine FingerPrint match.
- *And if* a corresponding User-Device association exists (User-Device association match).

Then based on these matches, the following four (out-of-box) combinations of conditions are possible:

- **Both, User-Device association and Machine FingerPrint, matched**
- **User-Device association matched, but Machine FingerPrint did not match**
- **User-Device association did not match, but Machine FingerPrint matched**
- **Both, User-Device association and Machine FingerPrint, did not match**



Note: Each of these rules is a combination of conditions that in conjunction with each other determine whether this rule has matched or not.

Add-On Rules

The out-of-box rules in RiskFort are generic and are configured for evaluating risk based on the rules that are applicable to all. If you need custom or industry-specific rules that are significantly different than those that RiskFort provides out-of-the-box, then you need to deploy *Add-On rules*.

Unlike Built-in rules, these rules are installed, but not deployed automatically.



Note: See [Chapter 12, “Working with Add-On Rules”](#) for detailed information on deploying with Add-On Rules.

Before an Add-On rule is deployed, its Rule Type must be configured by the Master Administrator. See [Chapter 6, “Preparing for Add-On Rules: Working with Rule Types”](#) for detailed information on how an MA can do so.

Evaluation Callout

Based on your business requirements, you can also write your own custom Evaluation rule, which will run at your application-end, outside of the RiskFort Server.

RiskFort executes this rule *after* all the Standalone and Add-On rules have been executed. This Callout accepts results of all previous rules and Additional Inputs as input and returns a response ([SUCCESS/FAILURE](#)), a *modifier string* (extra information to be used by the Scoring Callout), and an *annotation string* (the reason or the description returned back to RiskFort Server by your Callout implementation module).



Note: See [Chapter 9, “Configuring Callouts”](#) for more information on working with Evaluation Callouts.

Scoring Engine

In addition to Evaluation rules, RiskFort also provides **Scoring Engine** that accepts the input from the preceding Evaluation rules to generate the final Score and Advice.

Based on your business requirements, RiskFort also provides you the flexibility to add your own custom scoring logic in addition to RiskFort's standard scoring logic. You can do so with the help of **Scoring Callout**. By implementing a Scoring Callout, you can write your own custom scoring logic to process the Score, Advice, and risk-evaluation results generated by RiskFort's standard scoring program. The Scoring Callout will return the final risk Score, which can differ and will override the Score computed by RiskFort's standard scoring program.

Like Evaluation Callout, this is a custom rule that executes last, after the standard RiskFort scoring program and returns a final Score and Advice.



Note: See [Chapter 9, “Configuring Callouts”](#) for more information on working with Scoring Callouts.

Chapter 6

Preparing for Add-On Rules: Working with Rule Types



Important: All the configurations and tasks discussed in this chapter can *only* be performed by **Master Administrator**.

RiskFort uses *Rule Types* to define the capability and scope of the Add-On rules. For example, based on the type of the rule you are using, you can define an Add-On rule to look up the mapping or derived data from lists, use the User-Device association match and MFP match for evaluation, or perform numeric comparisons for evaluation purposes.

This chapter walks you through the basics of:

- [System-Defined Rule Types](#)
- [Working with Custom Rule Types](#)
- [Sample Input Definition XML](#)

System-Defined Rule Types

RiskFort is shipped with the following Rule Types that are pre-configured and can be used as-is. [Table 6-1](#) explains these rules.

Table 6-1. System-Defined Add-On Rule Types

Rule Type	Category	Rule Type Description
AMOUNT_CHECK	Numeric Comparison	If your Add-On rule needs to track transactions against a threshold amount in specified currency.
CARDHOLDER_MERCHANT_AMOUNT	Velocity	If your Add-On rule needs to track number (Frequency) of cardholder, merchant, and amount transactions within a specified period of time.

Table 6-1. System-Defined Add-On Rule Types

Rule Type	Category	Rule Type Description
COMBINATION RULE	Combination	If your Add-On rule uses the built-in RiskFort Rules and any Add-On rules that you might have defined earlier in conjunction with Logical Operators .
COUNTRY_LIST_LOOKUP	Simple List	If your Add-On rule needs to look up the default country list.
DERIVED_LIST_LOOKUP	Mapping (or Derived) List	If your Add-On rule needs to look up derived data from a Mapping (or Derived) List.
PREDECTIVE MODEL	RiskFort Model	If your Add-On rule needs input from the <i>RiskFort Predictive Model</i> for risk assessment.
PREDECTIVE MODEL SCORE ANALYSIS		Note: Before such an Add-On rule is configured, a model needs to be built. Contact Arcot Professional Services at services@arcot.com to build the model.
IPADDRESS_MERCHANT_AMOUNT	Velocity	If your Add-On rule needs to track the transaction amount at a specified merchant site.
IP_VELOCITY	Velocity	If your Add-On rule needs to track the number of transactions from a device within a specified period of time.
MERCHANT_CATEGORY_LOOKUP	Mapping (or Derived) List	If your Add-On rule needs to look up Merchant: Category mapping data from a Mapping (or Derived) List .
MERCHANT_REGION_LOOKUP	Mapping (or Derived) List	If your Add-On rule needs to look up Merchant: Region mapping data from a Mapping (or Derived) List.
NUMERIC_COMPARISON	Numeric Comparison	If your Add-On rule is based on numeric comparisons against a Threshold value.
SIMPLE_LIST_LOOKUP	Simple List	If your Add-On rule needs to look up data from a Simple List .
TRANSACTION_TYPE_CHECK	Simple List	If your Add-On rule also uses Arcot TransFort transaction types for risk evaluation.



Note: If you select *_LIST_LOOKUP as the rule type while configuring your Add-On rule, then a GA or an OA needs to upload the related look-up data.

See [“Uploading Add-On Rule List Data” in Chapter 12](#) for more information on how to do this.

The following sub-sections explain the Rule Type categories specified in [Table 6-1](#).

Numeric Comparison

This category enables you to compare two numeric expressions with the help of logical operators, such as Greater Than/[GT](#) (>), Greater Than or Equal To/[GTE](#) (>=), Equal To/[EQ](#) (=), Less Than/[LT](#) (<), Less Than or Equal To/[LTE](#) (<=), and Not Equal To/[NEQ](#) (!=).

Combination

This category enables you to combine out-of-the-box RiskFort rules and the deployed Add-On rules to build complex expressions with the help of logical operators (such as to [\(, \)](#), [AND](#), [OR](#), [NOT](#)).

RiskFort Model

RiskFort offers an advanced fraud modeling capability. Based on the historical data, this modelling capability can be built and created in RiskFort. By using the available transaction data and system data, the model generates a score that describes the extent to which the model suspects a transaction’s genuineness. This score typically ranges from [0](#) through [100](#), where the higher the number, the greater the possibility of fraud. RiskFort can be configured to send different responses to your calling application based on this model score.

The model score is available as a part of the system parameters (as ModelScore) while configuring Add-On Rules. This score can be used in conjunction with other data elements to arrive at a risk advice.

Velocity

This category extends the base User and Device Velocity rules that are shipped out-of-the-box. See [“Configuring User Velocity”](#) and [“Configuring Device Velocity” in Chapter 7](#) to understand the base Velocity rules.

Simple List

This dataset comprises simple data entries in the form of a list. For example, a list of countries considered safe falls under this category. Each entry in the list is separated from the other by the newline character, in the format:

```
<entry1>
<entry2>
.....
<entryn>
```

For example, the following list contains the names of the white-listed countries that are considered "safe":

```
Australia
Austria
Belgium
Canada
Denmark
Estonia
Finland
France
Germany
Greece
Iceland
Italy
Liechtenstein
Luxembourg
Montenegro
Netherlands
Norway
Portugal
Saudi Arabia
Singapore
```

```
Spain
Sweden
Switzerland
United Arab Emirates
United Kingdom
United States
Vatican
```

Mapping (or Derived) List

This dataset is derived from extensible elements passed by your application and comprises of complex data, in the form of name-value pairs.

For example, if you want to mark all transactions originating from merchants that belong to **Gambling** or **Adult Content** category as high-risk, then your Add-On rule must get the **Merchant** information, from which it should be able to derive the Group information, and then use this Group information to calculate the risk of the transaction. For this, the rule must have the access to the mapped or derived data.

Each entry in the list is separated from the other by the newline character, in the format. For example:

```
<name1, value1>
<name2, value2>
.....
<namen, valuen>
```

For example, the following list is in the **Merchant_Name, Category** format:

```
800florals, Flower Delivery
AdultReviews, Adult Content
Amazon, Online Shopping
American Airlines, Airline
BEST-BUY-DEAL, Online Shopping
British Airways, Airline
Casinogamblingweb, Gambling
```

```
Cliphunter, Adult Content
Costco, Online Shopping
eBay, Online Shopping
Emirates, Airline
Holiday Inn, Hospitality
JackpotFinder, Gambling
Kingfisher, Airline
Marriott, Hospitality
Ramada, Hospitality
Shopping.com, Online Shopping
SkyMall, Online Shopping
Taj, Hospitality
TWA, Airline
US Airways, Airline
Walmart, Online Shopping
Yellow Cab, Transportation
```

Working with Custom Rule Types

RiskFort also enables you to define and add any custom rule types, as per your business requirements.



Note: As a Master Administrator, you can add new rule types to RiskFort, while Global Administrators and Organization Administrators can then deploy these custom rule types to create new Add-On rules for the organizations in their purview.

This section guides you through the steps for:

- [Adding New Rule Types](#)
- [Viewing Existing Rule Types](#)

While adding a new rule type, you must provide an input definition XML file, which defines the rule parameters, attributes, and applicable name-value pairs. To demonstrate this, a sample XML file is also installed when you install RiskFort. The section, “[Sample Input Definition XML](#)” discusses this sample XML file.

Adding New Rule Types

To add a new rule type:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **Extensible Configurations** section, click the **Add Rule Type** link.

The Add Rule Type page ([Figure 6-1](#)) appears.

Figure 6-1 Add Rule Type Page

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo and 'Arcot Administration Console'. On the right, it says 'Welcome MASTERADMIN | Logout' and 'Last Login Time 06/15/2010 08:12:05 GMT'. Below the header is a navigation bar with tabs: 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (which is active), and 'Reports'. Under 'Services and Server Configurations', there's a sub-menu with 'RiskFort' and 'Administration Console'. The 'RiskFort' sub-menu is active, showing a sidebar with 'System Configuration' (including links to RiskFort Connectivity, Trusted Certificate Authorities, Protocol Configuration, and RiskFort Queueing Server Connectivity) and 'Extensible Configurations' (including 'Add Rule Type' and 'View Existing Rule Types'). The main content area is titled 'Add Rule Type' and contains the following text: 'Add new Add-On Rule Type to RiskFort. Note: Ensure that the Library Name does not contain the path or the extension.' Below this text are three input fields: 'Name of the Rule Type', 'Library Name (Without Extension)', and 'Input Definition XML'. There are 'Browse...' and 'Create' buttons next to the 'Input Definition XML' field.

5. Specify the type of the rule that you are creating in the **Name of the Rule Type** field.
6. Specify the file name (*without the extension and path*) of the library for the rule in the **Library Name** field.

This file *must* be available in the following directory:

- **For Windows:**

```
<install_location>\Arcot Systems\plugins\rules\addon\
```

- **For UNIX Platforms:**

```
<install_location>/arcot/plugins/rules/addon/
```

7. Click **Browse** to navigate to the location of the **Input Definition XML** file.

See [Sample Input Definition XML](#) that is shipped with RiskFort.

8. Click **Create** to create the specified Add-On rule type.
9. After the rule type has been added, navigate to the `\arcotadmin` directory on the appropriate location on your application server.

For example, on Apache Tomcat this location is:

```
<APP_SERVER_HOME>/arcotadmin/WEB-INF/classes/
```

10. Open the `riskfort-admin-message.properties` file using an editor.
11. Add the following lines to the file:

```
txt.riskserver.addonrule.$RULE_TYPE_NAME=$DISPLAYNAME
```

Here, `$RULE_TYPE_NAME` is the name of the rule type added and `$DISPLAYNAME` is the value that should be displayed on the screen (reports.)

For example:

```
txt.riskserver.addonrule.WhiteListedIp=White Listed IP
```

12. Save the changes and close the file.
13. Restart your application server, if required.

Viewing Existing Rule Types

RiskFort *does not* allow you to update an Add-On rule type that you added. However, you can view the [System-Defined Rule Types](#) or any custom rule types, which you added by using the Add Rule Type page ([Figure 6-1](#)).

To view the rule types that currently exist in the system:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **Extensible Configurations** section, click the **View Existing Rule Types** link.

The View Existing Rule Types page ([Figure 6-2](#)) appears.

Figure 6-2 View Existing Rule Types Page

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/15/2010 08:12:05 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports**

RiskFort | Administration Console

RiskFort

System Configuration

- [RiskFort Connectivity](#)
- [Trusted Certificate Authorities](#)
- [Protocol Configuration](#)
- [RiskFort Queueing Server Connectivity](#)

Extensible Configurations

- [Add Rule Type](#)
- View Existing Rule Types**

View Existing Rule Types

View existing Add-On Rule Types. Existing rule types cannot be updated.

Select Rule Type : --Select--

- Select the required Add-On rule type that you created from the **Select Rule Type** list.
The selected rule type details are displayed on the page (Figure 6-2.)

Figure 6-3 View Existing Rule Types Page

Arcot Administration Console

Welcome **MASTERADMIN** | [Logout](#)
Last Login Time 06/15/2010 08:12:05 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports**

RiskFort | Administration Console

RiskFort

System Configuration

- [RiskFort Connectivity](#)
- [Trusted Certificate Authorities](#)
- [Protocol Configuration](#)
- [RiskFort Queueing Server Connectivity](#)

Extensible Configurations

- [Add Rule Type](#)
- View Existing Rule Types**

View Existing Rule Types

View existing Add-On Rule Types. Existing rule types cannot be updated.

Select Rule Type : COUNTRY_LIST_LOOKUP

Parameter Name	Display Name	Type	Value If Predefined
RULETYPE	Rule Type	String	SIMPLE_LIST_LOOKUP
TAGNAME	Tag Name	String	RULESET.COUNTRY
MATCHTYPE	Match Type (EXACT or PARTIAL)	String	Exact
LOOKUPTYPE	Lookup Type (IN_LIST or NOT_IN_LIST)	String	IN_LIST
ENABLELISTCACHING	Enable List Caching (0 or 1)	Integer	1
LISTDATASET	List Data Set to Use	String	

Sample Input Definition XML

RiskFort is shipped with a sample XML file ([SampleAddonRuleType.xml](#)), which explains the general format of how to define an Add-On rule type and the parameters in that type.



Note: Currently only Text Box input fields are allowed. Contact the Arcot Technical Support (support@arcot.com) for further help.

This sample file is available at the following location:

For Windows:

`<install_location>\Arcot Systems\samples\addonruletype\`

For UNIX Platforms:

`<install_location>/arcot/samples/addonruletype/`

The [SampleAddonRuleType.xml](#) contains the following XML definition:

```
<ADDONTYPE>
  <NAME>MYNEWTYPE</NAME>
  <ORGNAME>DEFAULTORG</ORGNAME>
  <PARAMETER>
    <NAME>MerchId</NAME>
    <VALUE>MID</VALUE>
    <TYPE>1</TYPE>
    <ATTRIBUTE>
      <NAME>DISPNAME</NAME>
      <VALUE>Merchant ID</VALUE>
      <TYPE>1</TYPE>
    </ATTRIBUTE>
    <ATTRIBUTE>
      <NAME>DISPTYPE</NAME>
      <VALUE>TEXTBOX</VALUE>
      <TYPE>1</TYPE>
    </ATTRIBUTE>
  </PARAMETER>
</ADDONTYPE>
```

```

</ATTRIBUTE>
<ATTRIBUTE>
  <NAME>DISPROW</NAME>
  <VALUE>1</VALUE>
  <TYPE>2</TYPE>
</ATTRIBUTE>
</PARAMETER>
<PARAMETER>
  <NAME>ListID</NAME>
  <VALUE>LID</VALUE>
  <TYPE>1</TYPE>
  <ATTRIBUTE>
    <NAME>DISPNAME</NAME>
    <VALUE>List ID</VALUE>
    <TYPE>1</TYPE>
  </ATTRIBUTE>
  <ATTRIBUTE>
    <NAME>DISPTYPE</NAME>
    <VALUE>TEXTBOX</VALUE>
    <TYPE>1</TYPE>
  </ATTRIBUTE>
  <ATTRIBUTE>
    <NAME>DISPROW</NAME>
    <VALUE>2</VALUE>
    <TYPE>2</TYPE>
  </ATTRIBUTE>
</PARAMETER>
</ADDONTYPE>

```


Chapter 7

Managing Global Rule Configurations



Important: All the configurations and tasks discussed in this chapter can *only* be performed by **Global Administrators**.

You can manage RiskFort configurations at two levels:

- Global level, available to all organizations



Note: Although these rules are available to all organizations that are in scope of the GA who configured them, they cannot be used as-is at the organization-level. For example, even if you configure a Negative IP Address rule at the global level, individual organizations need to configure this rule either by copying from the global rule or by referring to the same.

- Organization level, available to individual organization

These configurations apply *only* to the specific organization where they were set.

Although you can change the default rule configurations individually for every organization in the system, but chances are that most of the organizations might be using the same configuration settings over and over again. Also, setting rule configurations for individual organizations can be a cumbersome task if there are large number of organizations configured. In this case, you might want to set the global configurations for the rules so that Organization Administrators (OAs) do not need to specify the same setting every time.



Note: The changes you make to the configuration globally or at organization-level are *not* applied automatically. You need to refresh all server instances to apply these configuration changes.

Managing global rule configurations is a key part of RiskFort management and optimization, and a key responsibility of Global Administrators. This chapter discusses global configurations and RiskFort rules that GAs can set as a "template" for *all* current and future organizations in the system. These configurations include:

- [Configuring Rulesets](#)
- [Configuring Trusted IP Addresses](#)
- [Configuring Trusted Aggregators](#)
- [Configuring Negative IP Addresses](#)
- [Configuring Negative IP Types](#)
- [Configuring Negative Country List](#)
- [Configuring User Velocity](#)
- [Configuring Device Velocity](#)
- [Configuring Zone Hopping](#)
- [Configuring Miscellaneous Rule Settings](#)



Note: These configurations are applicable for all organizations that are in the purview of the GA setting them. If you want to configure individual organizations, then you must log in as the Global Administrator (GA) or as Organization Administrator (OA) of the target organization to do so.

Refer to [Chapter 11, “Managing Organization-Specific RiskFort Configurations”](#) for more information.

In addition to these tasks, GAs can also:

- Configure the Basic Authentication Policy (see section, “[Specifying Basic Authentication Policy Settings](#)” on [page 2-32](#) for information on how to do this.)
- Change the Profile Information (see section, “[Changing Password and Profile Information](#)” on [page 2-23](#) for information on how to do this.)

Logging in as a Global Administrator

The first GA account *must* be created by MA. To log in as a GA and proceed with further configurations, you must obtain the account details from MA.

Before logging in, ensure that you have been communicated with your ID and the password that you will need to use to log in to your account for the first time. If for some reason you lose this password, then you must contact your administrator to regenerate it and send it to you again.

To log in to the Administration Console as a GA by using the basic Username-Password credentials:

1. Open a Web browser window.
2. Enter the URL to access Administration Console. The default Administration Console URL is:
<http://<hostname>:<port>/arcotadmin/adminlogin.htm>

Replace *hostname* and *port* in the preceding URL respectively with the host name or the IP address of the system where you have deployed the Administration Console and the port at which the console is listening.



Note: Arcot recommends that you bookmark this URL to access the Administration Console. Any GA, OA, or UA can use this URL to log in to the Administration Console by using their RiskFort Username-Password credentials.

The Administrator Login page appears, as shown in [Figure 7-1](#).

Figure 7-1 Administrator Login: Page 1

3. Enter the **Organization Name** that you want to log in to.



Important: *Do not* enter the **Display Name** of the organization. You must enter the unique ID of the organization (as defined by the Organization Name.) For example, if you want to log into the Default Organization, whose Display Name is Arcot Systems, then you must enter **defaultorg**, which is the (default) unique ID of this organization. You must *not* specify **Arcot Systems** here.

4. Click **Log In**.

The Login page shown in [Figure 7-2](#) appears.

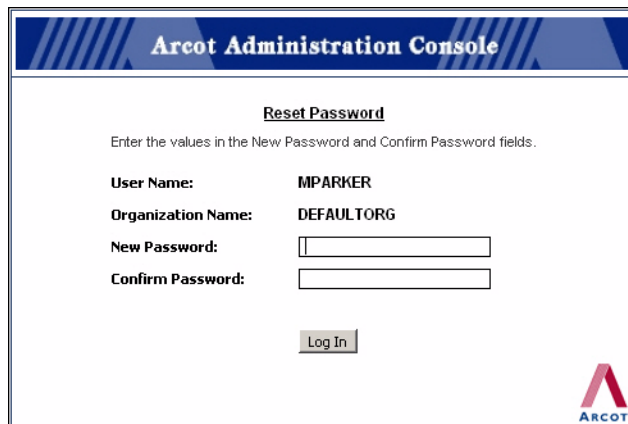
Figure 7-2 Administrator Login: Page 2



5. Specify the user ID in **User Name** field, enter the corresponding password that you were communicated in the **Password** field, and click **Log In**.

If you are logging in for the first time, you will be prompted to change the password, as shown in [Figure 7-3](#).

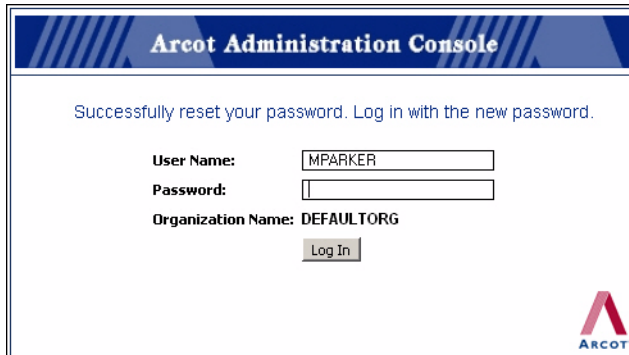
Figure 7-3 Administrator Login: Reset Password



6. Specify the **New Password**, **Confirm Password**, and then click **Log In**.

You will be redirected to the login page, as shown in [Figure 7-4](#).

Figure 7-4 Administrator Login: Page 2



Arcot Administration Console

Successfully reset your password. Log in with the new password.

User Name:

Password:

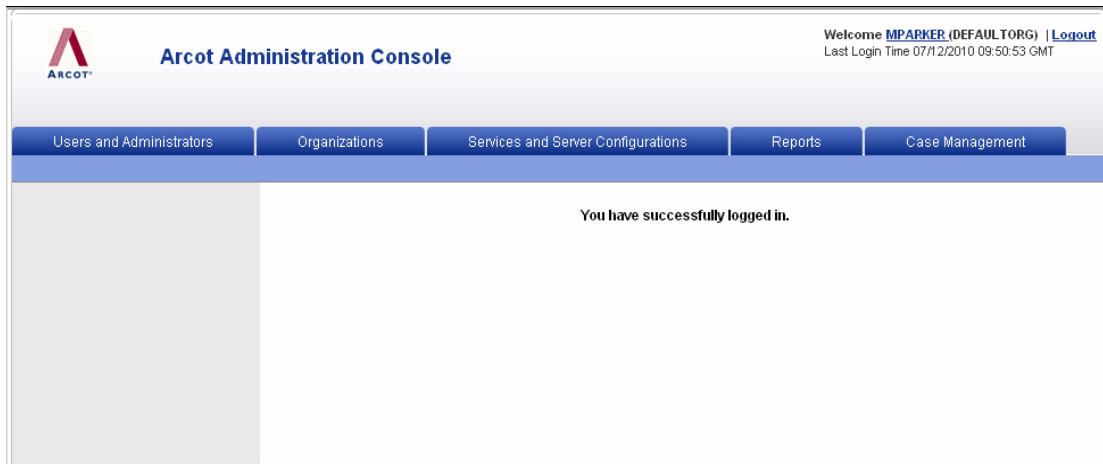
Organization Name: DEFAULTORG

ARCOT

7. Specify the **Password** again and click **Log In**.

The landing page of the Administration Console appears, as shown in [Figure 7-5](#).

Figure 7-5 Administrator: Successfully Logged In



Arcot Administration Console

Welcome [MPARKER \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators Organizations Services and Server Configurations Reports Case Management

You have successfully logged in.

Logging Out of the Administration Console

To log out of the Administration Console, click the **Logout** link in the console Header area, which is located at the top-right corner.

Security Recommendations While Using the Administration Console

To protect RiskFort from malicious attacks through the browser session, while using Administration Console, ensure that you:

- Do not share browser session with other applications.
- Do not open any other site while working with the Console.
- Enforce strict password restrictions for the Administration Console.
- Always log out after using the Administration Console.
- Close the browser window after the session is over.
- Assign proper roles to users according to the tasks they need to perform.

Configuring Rulesets

This section covers the following topics:

- [Understanding Rulesets](#)
- [Creating Rulesets](#)

Understanding Rulesets

A *ruleset* is a collection of one or more RiskFort rules ([Evaluation Rules](#) as well as [Scoring Engine](#)) that you have configured, along with their execution order and scoring priority. Each ruleset can be different from the other in terms of:

- Set of configured rules
- Score and priority for each rule in the set
- Enabling or disabling of rules in the set
- Configured parameters and data for each rule

As a GA, you can configure multiple global rulesets that are available to all the organizations that are within your scope. These rulesets can then be used by other GAs or OAs of these organizations to create new rulesets simply by "copying from" an existing ruleset. In addition, the "copied" rules within a ruleset can also be edited. This not only significantly saves the time and effort of individually configuring each rule again for organizations, but also reduces the number of errors.



Important: RiskFort is shipped with an out-of-box global ruleset called **DEFAULT**.

Creating Rulesets



Important: After you create a global ruleset as a Global Administrator (GA), the Organization Administrators (OAs) of the individual organizations must assign these rulesets to their respective organizations.

See [“Assigning Rulesets” on page 11-173](#) for more information on how to do this.

To create a ruleset:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Ruleset** section on the side-bar menu, click the **Create Ruleset** link.

The Create Ruleset page is ([Figure 7-6](#)) displayed.

Figure 7-6 Create Ruleset Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | **Administration Console**

RiskFort

Ruleset

- **Create Ruleset**

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Create Ruleset

*Creates Rulesets. Rulesets can be copied.
If the new ruleset does not copy some other ruleset, the ruleset will be created with factory settings.*

Name :

- Advanced Options

☐ Copy from an Existing Ruleset

Create

4. Specify the name of the ruleset in the **Name** field.
5. In the **Advanced Options** section, if required:
 - a. Select the **Copy from an Existing Ruleset** option, if you want to copy the rules configuration from an existing ruleset.
 - b. Select the name of the ruleset whose configuration you want to copy from the corresponding list.
6. Click **Create** to create and save the new ruleset.

The ruleset is yet not active, and not available to your end users.

7. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Trusted IP Addresses

In RiskFort, transactions that originate from or are routed through IP addresses and ranges that belong to the *Trusted IP address list* are considered low risk. As a result, RiskFort bypasses these transactions from risk evaluations and assigns them a low risk score and the `ALLOW` advice.

Use the Trusted IP/Aggregator Setup page, shown in [Figure 7-7](#), to perform the following tasks related to trusted IP addresses and ranges:

- [Adding a Trusted IP Address Range](#)
- [Updating a Trusted IP Address Range](#)
- [Deleting a Trusted IP Address Range](#)

Figure 7-7 Trusted IP/Aggregator Configuration Page

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo and 'Arcot Administration Console' title are visible. The top right corner shows a welcome message for 'MPARKER (DEFAULTORG)' with a 'Logout' link and the last login time '07/12/2010 09:50:53 GMT'. Below the header, there are navigation tabs: 'Users and Administrators', 'Organizations', 'Services and Server Configurations' (which is active), 'Reports', and 'Case Management'. Under 'Services and Server Configurations', there are sub-tabs: 'RiskFort' and 'Administration Console'. The left sidebar contains a 'RiskFort' section with links for 'Ruleset' (Create Ruleset), 'Rules' (Trusted IP/Aggregator, Negative IP Address, Negative IP Types, Negative Country List, User Velocity, Device Velocity, Zone Hopping, Add-On Rules, Callout Configuration, Miscellaneous Rule Configurations), 'Data Upload' (Upload List Data, Upload Mapping Data), 'Scoring' (Scoring Configuration), and 'Migrate to Production' (Migrate to Production). The main content area is titled 'Trusted IP/Aggregator Configuration' and contains the instruction: 'Select either Trusted IPs or Trusted Aggregators that you want to configure and click Next.' Below this instruction, there are two radio buttons: 'Trusted IPs' (which is selected) and 'Trusted Aggregators'. A 'Next' button is located at the bottom right of the main content area.

Adding a Trusted IP Address Range

To add a trusted IP address or range, perform the following tasks:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Trusted IP/Aggregator** link.

The Trusted IP/Aggregator Configuration page (Figure 7-7) is displayed.

4. Ensure that the **Trusted IPs** option is selected and click **Next**.

The Trusted IP Configuration Page appears.

5. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
6. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
7. If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The updated Trusted IP Configuration Page (Figure 7-8) appears.

Figure 7-8 Trusted IP Configuration Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted IP Configuration

Specify the range of IP addresses that are trusted. If this rule is scored first, then transactions originating from these IP addresses will receive an advice of Allow. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrtadmin` tool.

Update Existing Ruleset
SYSTEM - DEFAULT

Advanced Options

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

IP Address : [] . [] . [] . []

☒ **Subnet Mask :** [] . [] . [] . []

☐ **End IP Address :** [] . [] . [] . []

Add Range

Save Configuration

8. Specify the required **IP Address** that will be added to the Trusted IP List.
9. Specify one of the following:
 - **Subnet Mask:** If you want to specify a range of IP addresses based on the subnet mask to be added to the Trusted IP List.
 - **End IP Address:** If you want to specify a simple range of IP addresses to be added to the Trusted IP List.

- Click **Add Range** to add the IP address or range to the Trusted IP List.

The Trusted IP List table (Figure 7-9) (with the range that you just added) appears at the end of the page.

Figure 7-9 Trusted IP List

The screenshot shows a web interface titled "Trusted IP List". It contains a table with the following structure:

Select	IP Address	Subnet Mask	End IP Address
☐	156 . 120 . 59 . 28		156 . 120 . 60 . 10

Below the table are two buttons: "Delete" and "Update".

- Click **Save Configuration** to save the changes.

The changes are yet not active, and not available to your end users.

- To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Updating a Trusted IP Address Range

To update a trusted IP address or range:

- Complete [Step 1](#) through [Step 5](#) to display the *Trusted IP Configuration* page.
- Make the required changes in the **Trusted IP List** table.
- Select all the affected IP address range(s) in the **Trusted IP List** table.
- Click **Update** to update the changes that you made.
- Click **Save Configuration** to save the changes.

The changes are yet not active, and not available to your end users.

- To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Deleting a Trusted IP Address Range

To delete a trusted IP address or range, perform the following tasks:

- Complete [Step 1](#) through [Step 5](#) to display the *Trusted IP Configuration* page.

2. In the **Trusted IP List** table, select the required IP address range(s) that you want to delete.
3. Click **Delete** to delete the ranges that you selected.
4. Click **Save Configuration** to save the changes.

The changes are yet not active, and not available to your end users.

5. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Trusted Aggregators

Aggregators are third-party vendors who provide account aggregation services by collating login information of users across multiple enterprises. Many enterprises use the services of these account and data aggregation service providers to expand their online reach. The originating IP addresses when users log in from a protected portal versus when they come in through such aggregators are different.

Transactions originating from (or routed through) aggregators “trusted” to the organization are considered low-risk. For this purpose, RiskFort provides the ability to configure a list of these aggregators so that all transactions originating from the aggregators’ IP addresses are assigned a low risk-score, and the `ALLOW` advice.

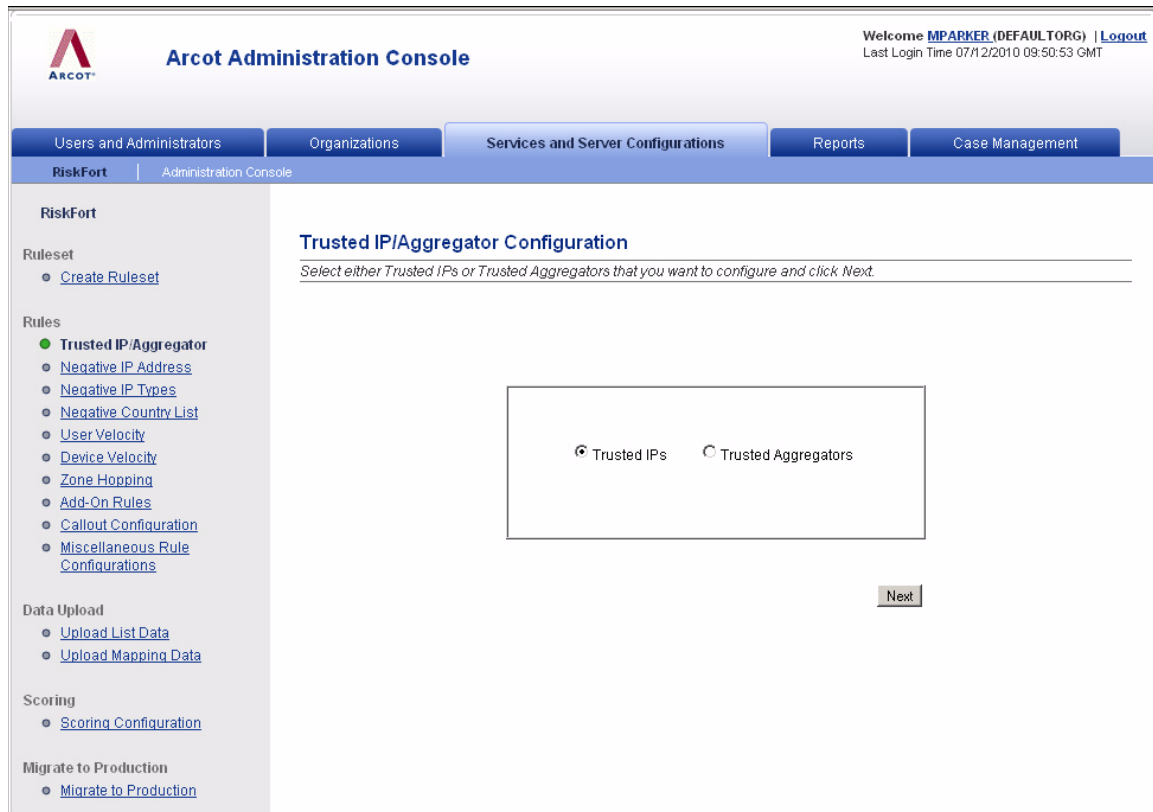
An aggregator’s IP is uniquely identified by RiskFort by using a combination of IP range and Aggregator ID. Using Administration Console, one Aggregator ID is issued per “trusted” Aggregator. This Aggregator ID must be sent to RiskFort along with the transaction.

RiskFort also enables you to specify up to *three* unique IDs for each aggregator at any time. This allows for the periodical rotation of the ID for the purpose of enhanced security. During this rotation, RiskFort continues to recognize the previous ID in addition to the new ID to allow update on the aggregator at a later time.

Use the Trusted IP/Aggregator Setup page, shown in [Figure 7-10](#), to perform the following tasks related to trusted aggregators:

- [Adding a Trusted Aggregator](#)
- [Updating a Trusted Aggregator](#)
- [Deleting a Trusted Aggregator](#)

Figure 7-10 Trusted IP/Aggregator Configuration Page



Adding a Trusted Aggregator

To add a trusted aggregator, perform the following tasks:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Trusted IP/Aggregator** link.

The Trusted IP/Aggregator Configuration page (Figure 7-10) is displayed.

4. Select the **Trusted Aggregators** option and click **Next**.

The Trusted Aggregator Configuration page appears.

5. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.

The updated Trusted Aggregator Configuration page, shown in [Figure 7-11](#), appears.

6. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
7. If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The updated Trusted Aggregators Configuration page ([Figure 7-11](#)) appears.

Figure 7-11 Trusted Aggregator Configuration Page

Arcot Administration Console

Welcome **MPARKER**(DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | **Administration Console**

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted Aggregator Configuration

Add a new aggregator that you trust or update the settings for an existing aggregator.

Update Existing Ruleset
SYSTEM - DEFAULT

Advanced Options

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name --Select--

Update Aggregator --Select--

Add Aggregator

Next

Save Configuration

- Specify the name of the new aggregator in the **Add Aggregator** field and click **Next**.
The updated Trusted Aggregator Configuration page, shown in the [Figure 7-12](#), appears.

Figure 7-12 Trusted Aggregator Configuration Page

Arcot Administration Console

Welcome **MPARKER** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted Aggregator Configuration

An aggregator is uniquely identified by using a combination of IP range and Aggregator ID. You can specify upto three unique IDs for each aggregator at any time. This enables you to periodically rotate or change the ID for the purpose of enhanced security. NOTE: RiskFort will continue to recognize the previous ID, in addition to the new ID to allow update on the aggregator at a later time.

Aggregator ID1 jsPKy5GG0jQuUxPVv3cf3I61JD0AwpNQlkrBIM4C+ZKsLJFUSAOM5g==

Aggregator ID2

Aggregator ID3

[Update Aggregator ID](#)

[Next](#)

- Click **Next** to continue.

The Trusted Aggregator Configuration page, as shown in [Figure 7-13](#), appears.

Figure 7-13 Trusted Aggregator Configuration Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Trusted Aggregator Configuration

Specify the range of IP addresses that are assigned to an aggregator. If this rule is scored first, then transactions originating from these IP addresses will receive an advice of Allow. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrtadmin` tool.

Aggregator: HSBC

IP Address : . . .

☒ **Subnet Mask :** . . .

☐ **End IP Address :** . . .

[Add Range](#)

10. On the Trusted Aggregator Configuration page:

- Enter the starting IP Address in the **IP Address** field.
- Select one of the following options:
 - Subnet Mask:** If you want to specify a range of IP addresses based on the subnet mask to be added to the Trusted IP List.
 - End IP Address:** If you want to specify a simple range of IP addresses to be added to the Trusted Aggregator List.
- Click **Add Range** to add this IP address or range to the database.

The Trusted IP List table (Figure 7-14) with the range that you just added for the aggregator appears at the end of the page.

Figure 7-14 Trusted IP List for the Aggregator

Trusted IP List			
Select	IP Address	Subnet Mask	End IP Address
☐	197 . 139 . 182 . 131	255 . 255 . 252 . 0	. . .
Delete Update			

The changes are yet not active, and not available to your end users.

- To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Updating a Trusted Aggregator

RiskFort enables you to update the Aggregator IDs. The periodic update of these IDs is referred to as *rotation of Aggregator IDs*.



Important: Arcot strongly recommends periodic rotation or change of the Aggregator IDs for security purposes. You can decide this rotation duration according to your business rules.

After an ID is updated, you must ensure that the latest Aggregator ID is conveyed to the aggregator. There might be a delay in propagating the Aggregator IDs. In this duration, RiskFort recognizes the old, as well as the new Aggregator ID associated with the IP address.



Note: The transactions originating from the aggregator-end must contain this aggregator ID in the form specified by RiskFort APIs.

To update an aggregator ID:

- Complete [Step 1](#) through [Step 5](#) to display the *Trusted Aggregator Configuration* page.
- Select an existing aggregator from the **Update Aggregator** list and click **Next**.

The Trusted Aggregator Configuration page, shown in [Figure 7-12](#), with the Aggregator ID(s) for the selected aggregator appears.

- Click **Update Aggregator ID** to generate a new Aggregator ID.

The updated Aggregator ID(s) for the aggregator appears and the next empty Aggregator ID is displayed, as shown in [Figure 7-15](#).

Figure 7-15 Trusted Aggregator Configuration Page

The screenshot shows the Arcot Administration Console interface. The top navigation bar includes links for Users and Administrators, Organizations, Services and Server Configurations (selected), Reports, and Case Management. The left sidebar contains links for RiskFort, Ruleset (Create Ruleset), Rules (Trusted IP/Aggregator, Negative IP Address, Negative IP Types, Negative Country List, User Velocity, Device Velocity, Zone Hopping, Add-On Rules, Callout Configuration, Miscellaneous Rule Configurations), Data Upload (Upload List Data, Upload Mapping Data), Scoring (Scoring Configuration), and Migrate to Production (Migrate to Production).

The main content area is titled "Trusted Aggregator Configuration". It contains a text box with the following text: "An aggregator is uniquely identified by using a combination of IP range and Aggregator ID. You can specify upto three unique IDs for each aggregator at any time. This enables you to periodically rotate or change the ID for the purpose of enhanced security. NOTE: RiskFort will continue to recognize the previous ID, in addition to the new ID to allow update on the aggregator at a later time." Below this text is a table with three columns: Aggregator ID1, Aggregator ID2, and Aggregator ID3. The table contains the following values:

Aggregator ID1	Aggregator ID2	Aggregator ID3
4p3q/9QMj0qGivG2LpW1aX+AhF9717c	/aAukD7bm55y55Wb+SUcceg==	jSPKy5GG0jQuUxPV3cf3l61JDcAwPnQlkrBIM4C+ZKsLJFUSAOM5g==

Below the table is an "Update Aggregator ID" button. At the bottom right of the main content area is a "Next" button.

- Click **Next** to continue.

The Trusted Aggregator Configuration page ([Figure 7-13](#)) appears. This page enables you to update the IP address, range, or subnet mask for the specified IP address or range, if required.

- In the **Trusted IP List** section, select the aggregator IP addresses or ranges you want to update.
- Make the required changes and click **Update**.

The changes are yet not active, and not available to your end users.

- To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Deleting a Trusted Aggregator

To delete a trusted aggregator, perform the following tasks:

1. Complete [Step 1](#) through [Step 5](#) to display the *Trusted Aggregator Configuration* page.
2. Select an existing aggregator from the **Update Aggregator** list and click **Next**.
The Trusted Aggregator Configuration page ([Figure 7-12](#)) for updating the Aggregator ID appears.
3. Click **Next**
The Trusted Aggregator Configuration page ([Figure 7-13](#)) for updating the IP address ranges is displayed.
4. In the **Trusted IP List** section, select the aggregator IP addresses or ranges you want to delete.
5. Click **Delete** to delete the selected information.
The changes are yet not active, and not available to your end users.
6. To make the changes active, you must migrate them to production.
Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Negative IP Addresses

The *Negative IP address list* is a collection of IP addresses that have been the origin of known anonymizer proxies or fraudulent and malicious transactions in the past. This list is the source of the [Negative](#) category discussed in the [“Configuring Negative IP Types”](#) section.

Use the Negative IP Address List page, as shown in [Figure 7-16](#), to configure the negative IP address ranges for your organization.

Figure 7-16 Negative IP Address List Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- Negative IP Address**
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Negative IP Address List

Add to a list of Negative IP Address Range. Negative IP ranges can be added along with specifying whether the end IP address is a mask or an IP. Also one can specify the type of range added. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrfdadmin` tool.

Update Existing Ruleset
SYSTEM - DEFAULT

Advanced Options

☒ Use Own
 ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Upload Negative IP Ranges

☒ Append
 ☐ Replace

Upload Data File: [Browse...](#)

[Upload](#)

Add/Delete Negative IP Range

IP Address: . . .
☒ Subnet Mask: . . .
☐ End IP Address: . . .

Information Source:

[Add Range](#) [Delete Range](#)

[Save Configuration](#)

Adding or Deleting IP Address Ranges

To add or delete negative IP addresses and ranges for your organization:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Negative IP Addresses** link.

The Negative IP Address List page is displayed.

4. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.

The configuration information for the specified ruleset appears.

5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The updated page appears ([Figure 7-16.](#))

7. In the *section under Advanced Options*:
 - a. Enter the starting IP address in the **IP Address** field.
 - b. Select one of the following options:
 - **Subnet Mask:** If you want to specify a range of IP addresses based on the subnet mask to be added to the Negative IP Address List.
 - **End IP Address:** If you want to specify a simple range of IP addresses to be added to the Negative IP Address List.

- c. Specify the **Information Source** (or vendor) of the negative IP address range.
8. Click one of the following buttons, as required:
 - **Add Range:** To add the specified IP address or range to the database.
 - **Delete Range:** To delete the specified IP address or range from the database.

The appropriate message will be displayed.

The changes are yet not active, and not available to your end users.

9. To make the changes active, you must migrate them to production.

Refer to [““Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Negative IP Types

RiskFort uses the IP address of the user’s computer as one of the input parameters to assess the risk of each transaction. RiskFort evaluates the incoming transaction and checks if it originated from an IP address marked as *negative type*. Such transactions are typically denied. The different categories of negative types are:

- **Negative**

IP addresses with this designation have been sources of fraudulent transactions in the past.



Important: Use this option, if you manually configured an IP addresses as negative in the Add Negative IP Address page, as discussed in [“Configuring Negative IP Addresses”](#).

- **Active**

IP addresses with this designation allegedly are anonymizing proxies that have been sources of fraudulent transactions and have been active in the last six months.

- **Suspect**

IP addresses with this designation allegedly are anonymizing proxies that have been active over the last two years, but not for the last six months.

- **Private**

IP addresses with this designation allegedly are anonymizing proxies that are not publicly accessible. These addresses typically belong to commercial ventures that sell anonymity services to the public.

- **Inactive**

IP addresses with this designation allegedly have been sources of fraudulent transactions, but have been found inactive in the last two years.

- **Unknown**

IP addresses with this designation allegedly are anonymizing proxies for which no positive results are available currently.



Note: The Active, Suspect, Private, Inactive, and Unknown negative type categories are derived from the Quova data.

Use the Negative IP Types Configuration page, as shown in the [Figure 7-17](#), to configure the type of negative IP addresses applicable for your organization.

Figure 7-17 Negative IP Types Configuration Page



Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
 Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators

Organizations

Services and Server Configurations

Reports

Case Management

RiskFort

Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- **Negative IP Types**
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Negative IP Types Configuration

Select the IP Types that RiskFort will use to determine whether an incoming IP address is negative or not. For the changes to take effect, migrate them to production and refresh the server cache by running the **arradmin** tool.

Update Existing Ruleset

SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own

☐ Copy from an Existing Ruleset

☐ Refer an Existing Ruleset

Ruleset Name

--Select--

IP Type	Default	Active	Proposed
Negative <i>Negative IP addresses that you have manually configured.</i>	☒	☒	☒
Active <i>Anonymizers that have tested positive within the last six months.</i>	☒	☒	☒
Suspect <i>Anonymizers that have tested positive within the last two years, but not the last six months.</i>	☒	☒	☒
Private <i>Anonymous proxies that are not publicly accessible.</i>	☒	☒	☒
Inactive <i>Anonymizers that have not tested positive within the last two years.</i>	☐	☐	☐
Unknown <i>Anonymizers for which no positive test results are currently available.</i>	☐	☐	☐

Save

To configure the types of negative IP addresses applicable to your organization:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Negative IP Types** link.

The Negative IP Types Configuration page is displayed.

4. From the **Update Existing Ruleset** list, select the ruleset that for which this configuration is applicable.

The configuration information for the specified ruleset appears.

5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The *updated* Negative IP Types Configuration page, shown in [Figure 7-17](#), appears.

7. In the **Proposed** column, select the applicable types of negative IP address category against each **IP Type**.
8. Click **Save** to save the changes.

The changes are yet not active, and not available to your end users.

9. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Negative Country List

Negative Country list comprises all countries from which fraudulent or malicious transactions are known to have originated in the past. Enterprises may also maintain this list in line with the regulations of their country.

RiskFort derives the country information based on the input IP address. It, then, uses this data to score the potential for fraud for online transactions originating from such countries. For this purpose, RiskFort also integrates with Quova, which enhances the analysis by providing detailed geographic information for each IP address by mapping it to a region.

To know more about Quova and their services, go to:

<http://www.quova.com>

RiskFort evaluates the incoming transactions and checks if these transactions originated from an IP address that belongs to a country marked as negative. Such transactions are typically denied.

Use the Negative Country List page, shown in [Figure 7-18](#), to add a country to the Negative Country list or remove a country from the list.

Figure 7-18 Negative Country List Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Log](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | **Administration Console**

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- Negative Country List**
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Negative Country List

Add or update the list of countries that have been source of high-risk transactions. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrfadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

Advanced Options

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Available Countries

AFGHANISTAN
ALAND ISLANDS
ALBANIA
ALGERIA
AMERICAN SAMOA
ANDORRA
ANGOLA
ANGUILLA
ANTARCTICA
ANTIGUA AND BARBUDA

Selected Countries

Save

To update the Negative Country List:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Negative Country List** link.

The Negative Country List page is displayed.

4. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The *Update Negative Country List* page is displayed, as shown in [Figure 7-18](#).

7. Select the countries that you want to add from the **Available Countries** list to the **Selected Countries** list.
8. Click the **>** or **<** buttons to move selected countries to the desired list. You can also click the **>>** or **<<** buttons to move all countries to the desired lists.



Note: Hold the **Ctrl** key to select more than one country at a time.

9. Click **Save** to save the changes.

The changes are yet not active, and not available to your end users.

10. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring User Velocity

The ***User Velocity rule*** keeps a check on the number of transactions from a user within a specified period of time. It is based on the following parameters:

- **Number of Risk Evaluations per User**
Denotes the number of transactions (**N**) performed by RiskFort for a specified user, irrespective of the Advice or Risk Score.
The default value for this parameter is **5**.
- **Time Interval**
Denotes the time period (**T**) in which the number of transactions are being tracked.
The default value for this parameter is **60**.
- **Unit for Time Interval**
Denotes the unit in which the time period (**T**) is measured in.
The default value for this parameter is **Minutes**.

Use the User Velocity Configuration page, shown in [Figure 7-19](#), to configure this rule.

Figure 7-19 User Velocity Configuration Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- User Velocity**
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

User Velocity Configuration

Specify the maximum number of successive transactions allowed from the same user in the specified interval of time. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrtadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Parameter	Default	Active	Proposed
Number of Risk Evaluations per User	5	5	5
Time Interval	60	60	60
Unit for Time Interval	MINUTES	MINUTES	MINUTES

[Save](#)

To configure the User Velocity rule:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **User Velocity** link.

The User Velocity Configuration page is displayed.

4. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, in the **Advanced Options** section select *one* of the following options:
 - **Use Own:** If you select this option, then you can specify your own configuration values.
 RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.
 Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.
 - **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.
 To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The updated User Velocity Configuration page appears, as shown in [Figure 7-19](#).

7. In the table on the page:
 - a. Specify the **Proposed** value for the **Number of Risk Evaluations per User** parameter.
 - b. Specify the **Proposed** value for the **Time Interval** parameter.
 - c. Select the **Proposed** unit for the **Unit for Time Interval** parameter.
 This value denotes the maximum number of transactions (within the specified time interval) for a user that is considered safe. If the actual number of transactions within the specified time exceeds this number, then RiskFort will track it as a risk, which will result in the matching of the User Velocity rule.
8. Click **Save** to save the changes.
 The changes are yet not active, and not available to your end users.
9. To make the changes active, you must migrate them to production.
 Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Device Velocity

The ***Device Velocity rule*** keeps a check on the number of transactions from a device within a specified period of time. It is based on the following parameters:

- **Time Interval**

Denotes the time period (**T**) in which the number of transactions are being tracked.

The default value for this parameter is **60**.

- **Unit for Time Interval**

Denotes the unit in which the time period (**T**) is measured in.

The default value for this parameter is **Minutes**.

- **Number of Risk Evaluations per Device**

Denotes the number of transaction (**M**) performed by RiskFort for a specified device, irrespective of the fact whether the risk evaluation resulted in success or failure.

The default value for this parameter is **10**.

Use the Device Velocity Configuration page, shown in [Figure 7-20](#), to configure this rule.

Figure 7-20 Device Velocity Configuration Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

RiskFort | **Administration Console**

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- Device Velocity**
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Device Velocity Configuration

*Specify the maximum number of successive transactions allowed from the same enduser-device in the specified interval of time. For the changes to take effect, migrate them to production and refresh the server cache by running the **arrfadmin** tool.*

Update Existing Ruleset
SYSTEM - DEFAULT

Advanced Options

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name --Select--

Parameter	Default	Active	Proposed
Number of Risk Evaluations per Device	10	10	10
Time Interval	60	60	60
Unit for Time Interval	MINUTES	MINUTES	MINUTES

Save

To configure the Device Velocity rule, perform the following steps:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Device Velocity** link.

The Device Velocity Configuration page is displayed.

4. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The updated Device Velocity Configuration page appears, as shown in [Figure 7-20](#).

7. In the table on the page:
 - a. Specify the **Proposed** value for the **Number of Risk Evaluations per Device** parameter.
 - b. Specify the **Proposed** value for the **Time Interval** parameter.
 - c. Specify the **Proposed** unit for the **Unit for Time Interval** parameter.

This value denotes the maximum number of transactions (within the specified time interval) for a device that is considered safe. If the actual number of transactions within the specified time exceeds this number, then RiskFort will track it as a risk, which will result in the matching of the Device Velocity rule.

8. Click **Save** to save the changes.

The changes are yet not active, and not available to your end users.

9. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Zone Hopping

Zone hopping tracks successive transactions from the same user that occur at distant locations (separated by large distances) at a speed beyond what is reasonably possible within a short time span. For example, if Bob logs from New York at 9 AM (GMT) and again from London at 10 AM (GMT), then Zone Hopping rule will track the latter transaction as risky.

The Zone hopping rule is based on the following parameters:

- **Maximum Speed at which a User can Travel**

Denotes the maximum speed (S, in miles per hour) with which a user can physically travel using conventional transport, such as airplanes, cars, and trains.

If the speed with which a user appears to have moved (in the time frame between two successive transactions) exceeds this pre-configured threshold speed (S), then RiskFort considers it as a case of zone hopping.

By default this value is 500 miles, but you can configure it by setting the value of **Maximum Speed at which a User can Travel** field in the Zone Hopping Configuration page.

- **Maximum Number of Users Sharing the Same User ID**

Sometimes, multiple users (for example, husband and wife) can use the same user name. In such cases, there is a possibility that they might be located in different zones. In such cases, RiskFort must not consider this as a case of Zone hopping. For example, if husband logs in from New York at 10 AM (GMT) and wife from London at 11 AM (GMT), then RiskFort will not mark these transactions as risky.

By default this value is 1, but you can configure it to 2 by editing the **Maximum Number of Users Sharing the Same Username** field in the Zone Hopping Configuration page.

- **Maximum Distance Tolerance for IP Address Locations**

Because of variation in location of the IP address provided by ISPs, a user's physical location (geographic latitude and longitude) cannot be determined to a high level of precision by using their public IP address. To address this, RiskFort uses an uncertainty offset (U, in miles) to accommodate the variation in the physical location of the IP address from which the transaction originated.

By default this variation is about 50 miles, but you can configure it by setting the value of **Maximum Distance Tolerance for IP Address Location** field in the Zone Hopping Configuration page.

Use the Zone Hopping Configuration page ([Figure 7-21](#)), to configure this rule.

Figure 7-21 Zone Hopping Configuration Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- Zone Hopping**
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Zone Hopping Configuration

If multiple transactions from a single user are originating from different geographic locations in quick succession, specify the speed at which the user can possibly travel. Also specify if the user account is shared between two people. For the changes to take effect, migrate them to production and refresh the server cache by running the `arrfadmin` tool.

Update Existing Ruleset
SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Parameter	Default	Active	Proposed
Maximum Speed at which a User can Travel (Miles per Hour)	500	500	500
Maximum Number of Users Sharing the Same User ID	1	1	1
Maximum Distance Tolerance for IP Address Locations (Miles)	50	50	50

[Save](#)

To configure the Zone Hopping rule:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Zone Hopping** link.

The Zone Hopping Configuration page is displayed.

4. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, in the **Advanced Options** section select *one* of the following options:
 - **Use Own:** If you select this option, then you can specify your own configuration values.
 RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.
 Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.
 - **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.
 To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The updated Zone Hopping Configuration page appears, as shown in [Figure 7-21](#).

7. Specify the **Proposed** value for the **Maximum Speed at which a User can Travel** parameter.
8. Specify the **Proposed** value for the **Maximum Number of Users Sharing the Same User ID** parameter.
9. Specify the **Proposed** value for the **Maximum Distance Tolerance for IP Address Locations** parameter.
10. Click **Save** to save the changes.

The changes are yet not active, and not available to your end users.

11. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Miscellaneous Rule Settings

You must first understand the [Related Concepts](#) before you proceed with [Specifying Miscellaneous Rule Configurations](#), which includes **User Creation Mode** and **Machine FingerPrint Threshold**, for your system.

Use the Miscellaneous Rule Configurations page ([Figure 7-22](#)) to specify the required user creation mode.

Related Concepts

For correctly specifying information in the Miscellaneous Rule Configurations page ([Figure 7-22](#)) page, you must understand:

- [User Creation Mode](#)
- [Machine FingerPrint \(MFP\) Threshold](#)

User Creation Mode

Users can be created in RiskFort database by using one of the *user creation modes* discussed in the following sub-sections:

Explicit User Creation Mode

In this case, you would need to explicitly call the `createUser()` API to create your users in the RiskFort *before* you can do a risk evaluation (by calling the `evaluateRisk()` API) for their transactions.

If you call `evaluateRisk()` before creating the user, then RiskFort's Known User Rule ([Chapter 5, "Understanding RiskFort Rule Basics"](#)) will not match resulting in the `ALERT` risk advice.

Implicit User Creation Mode

If you have configured user creation mode as *Implicit*, then you do not need to invoke the `createUser()` API for creating users in RiskFort. In this case, when you call the `evaluateRisk()` API for a transaction, RiskFort will automatically create the user (if not already present) in the RiskFort.

If the user was not present before, then when `evaluateRisk()` is called for the first time for the specified user, RiskFort will not match the User Known Rule and return the `ALERT` advice. For all subsequent calls to `evaluateRisk()` for this user, RiskFort will determine this user to be already present in the RiskFort database, and therefore the rule will match.

Machine FingerPrint (MFP) Threshold

To develop a risk profile in real time, and then generate a corresponding Risk Score and Advice, RiskFort collects a large range of information from the end-user device that is being used by the user for the current transaction. This information can be classified into a number of categories, such as:

- Operating system information
- Browser information
- Screen settings
- User preferences

This information is referred to as Machine FingerPrint (MFP) or device signature. For every transaction by a specified user, RiskFort matches the stored MFP with the incoming MFP. If this match percentage (%) is equal to or more than the value specified in the System Configuration screen, then it is considered "safe".

Specifying Miscellaneous Rule Configurations

To specify the user creation mode and the MFP threshold percentage:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Miscellaneous Rule Configurations** link.

The Miscellaneous Rule Configurations page is displayed.

4. From the **Update Existing Ruleset** list, select the ruleset that for which this configuration is applicable.

The configuration information for the specified ruleset appears.

5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, in the **Advanced Options** section select *one* of the following options:
 - **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The configuration table for the specified ruleset appears, as shown in [Figure 7-22](#).

Figure 7-22 Miscellaneous Rule Configurations Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators | Organizations | **Services and Server Configurations** | Reports | Case Management

RiskFort | Administration Console

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- Miscellaneous Rule Configurations**

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Miscellaneous Rule Configurations

Specify the mode in which users will be created in RiskFort database and the the Machine FingerPrint (MFP) match percentage at which a user transaction will be considered safe. The changes that you make on this page will not be effective unless you migrate them to production and refresh the server cache by running the `arrfadmin` tool.

Update Existing Ruleset

SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own
 ☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name: --Select--

Parameter	Default	Active	Proposed
User Creation Mode	Explicit	Explicit	☐ Implicit ☒ Explicit
Machine FingerPrint (MFP) Threshold, in Percentage	50	50	50

Save

- Under the **Proposed** column, select the required option (**Implicit** or **Explicit**) for the **User Creation Mode**.
- Under the **Proposed** column, specify the required value for the **Machine FingerPrint (MFP) Threshold, in Percentage** option.
- Click **Save** to save the changes.

The changes are yet not active, and not available to your end users.

10. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Chapter 8

Configuring Scoring

This chapter describes how to configure RiskFort scoring to meet your business requirements. After you update any of the **default** (out-of-box) configurations for RiskFort, the changes are not immediately **active** (available to your end users.) You *must* use the **Migrate to Production** link in the side-bar menu of the Administration Console to "move" all **proposed** configuration changes to your production database. See the [“Migrating to Production”](#) section to understand the concept of *default*, *proposed*, and *active* configuration data used by RiskFort.

This chapter covers:

- [Understanding RiskFort Scoring](#)
- [Configuring Scoring](#)
- [Migrating to Production](#)



Note: The administrator performing configuration-related activities *must have* privileges to perform these operations. For more information on the privileges available to administrators at each level, refer to the section, [“Summary of Administrative Privileges”](#) in Chapter 1.

Understanding RiskFort Scoring

For each risk evaluation request from your application, RiskFort executes [Evaluation Rules](#) to generate a *Risk Score* (or *Score*). This Score is typically a value from 0 through 100 that maps to a recommended *Risk Advice* (or *Advice*.) RiskFort then uses the [Scoring Engine](#) to generate the final Score and the corresponding Advice.

[Table 8-1](#) explains the mapping between the pre-defined score value ranges and the corresponding Advice.

Table 8-1. Risk Advice Matrix

Score Value (From)	Score Value (To)	Advice	Default Recommended Action
0	30	ALLOW	Allow the transaction to proceed.
31	50	ALERT	Take an appropriate action. For example, if the user name is currently unknown, then on getting an alert you can either redirect it to a CSR or you can create a user in RiskFort.
51	70	INCREASEAUTH	Perform additional authentication before proceeding any further.
71	100	DENY	Deny the transaction.

Configuring Scoring

Use the Scoring Configuration page shown in following figure ([Figure 8-1](#)) for:

- Enabling or disabling the out-of-box rules, Add-On rules, and Callouts
- Configuring the risk score and scoring priority of the rules

Figure 8-1 Scoring Configuration Page

Scoring Configuration

Enable or disable rules for execution and scoring, and configure the risk score and scoring priority of each rule. The Default Score is used, if none of the rules in the first table matched.

Update Existing Ruleset

SYSTEM - DEFAULT

- Advanced Options

☐ Copy from an Existing Ruleset --Select--

RULENAME	ACTIVE				PROPOSED				
	Enabled Execution	Enabled Scoring	Risk Score	Priority	Enabled Execution	Enabled Scoring	Risk Score	Advice	Priority
Exception User Check	☒	☒	30	10	☒	☒	30	ALLOW	↓
Negative IP Check	☒	☒	100	20	☒	☒	100	DENY	↑ ↓
Negative Country Check	☐	☐	100	30	☐	☐	100	DENY	↑ ↓
Trusted IP/Aggregator Check	☒	☒	30	40	☒	☒	30	ALLOW	↑ ↓
Unknown User Check	☒	☒	50	50	☒	☒	50	ALERT	↑ ↓
DeviceID Check	☒	☒	65	60	☒	☒	65	INCREASEAUTH	↑ ↓
User Velocity Check	☒	☒	65	70	☒	☒	65	INCREASEAUTH	↑ ↓
Device Velocity Check	☒	☒	65	80	☒	☒	65	INCREASEAUTH	↑ ↓
Zone Hopping Check	☐	☐	65	90	☐	☐	65	INCREASEAUTH	↑ ↓
User Associated with Device and Device-MFP Matched	☒	☒	10	100	☒	☒	10	ALLOW	↑ ↓
Device-MFP Matched but User Not Associated with Device	☒	☒	65	110	☒	☒	65	INCREASEAUTH	↑ ↓
User Associated with Device but Device-MFP Does Not Match	☒	☒	65	120	☒	☒	65	INCREASEAUTH	↑ ↓
User Not Associated with Device and Device-MFP Does Not Match	☒	☒	65	130	☒	☒	65	INCREASEAUTH	↑

	ACTIVE	PROPOSED
DEFAULT SCORE	30	30

Save

To enable or disable rules and to configure the risk score and scoring priority of rules:

1. Ensure that you are logged in as a GA or as an OA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Scoring** section on the side-bar menu, click the **Scoring Configuration** link.

The Scoring Configuration page appears.

4. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.

The configuration information for the specified ruleset appears, as shown in [Figure 8-1](#).

5. If required, expand the **Advanced Options** section by clicking the **[+]** sign.
6. If required, select the **Copy From an Existing Ruleset** option from the **Advanced Options** section and then select the name of the ruleset whose configuration you want to copy from the list.

If you select this option, then you can copy the configuration from an existing ruleset and modify it, as required.



Note: The changes that you make on this page will *not* affect the ruleset that you are copying from.

7. For each rule, in the **Proposed** column of the displayed table:
 - a. Select (to enable the rule) or clear (to disable the rule) the **Enabled Execution** option.
 - b. Select (to enable the scoring of the rule) or clear (to disable the scoring of the rule) the **Enabled Scoring** option.
 - c. Specify the required **Risk Score**.
 - d. Click the Up (↑) arrow to increase the relative scoring **Priority** or the Down arrow (↓) to decrease the same.
8. In the **PROPOSED** column for **DEFAULT SCORE** (the second table on the page), specify the required **Risk Score**.



Note: RiskFort will use this value to generate the final Risk Score and Advice if *none* of the rules in the preceding table match.

9. Click **Save** to save the changes you made on this screen.

The changes are yet not active, and not available to your end users.

10. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Migrating to Production

RiskFort is shipped with **default** (out-of-box) settings for the following rules and configurations:

- Trusted IP Address and Aggregators
- Negative IP Address
- Negative IP Types
- Negative Country List
- User Velocity
- Device Velocity
- Zone Hopping
- Miscellaneous Rule Configurations
- Scoring

In addition, you can also configure:

- Add-On Rules
- Callouts

When the data related to the preceding lists is being configured, it is referred to as *Proposed data*. This data can be created over a period of time by using several administrative sessions. While you configure this data, it is stored as *Proposed configuration* area and is reflected in the **Proposed** column on respective configuration page. As a result, any changes that you make to the **Proposed** column affect this data.

When all data is configured according to your requirements, then the Proposed data can be converted to *Active data* (the **Active** column on respective configuration page) by migrating it to production and refreshing the RiskFort Server cache using the [arrfadmin: Server Refresh and Shutdown Tool](#) tool.



Note: At any point in time, RiskFort Servers work with Active data configurations *only*.

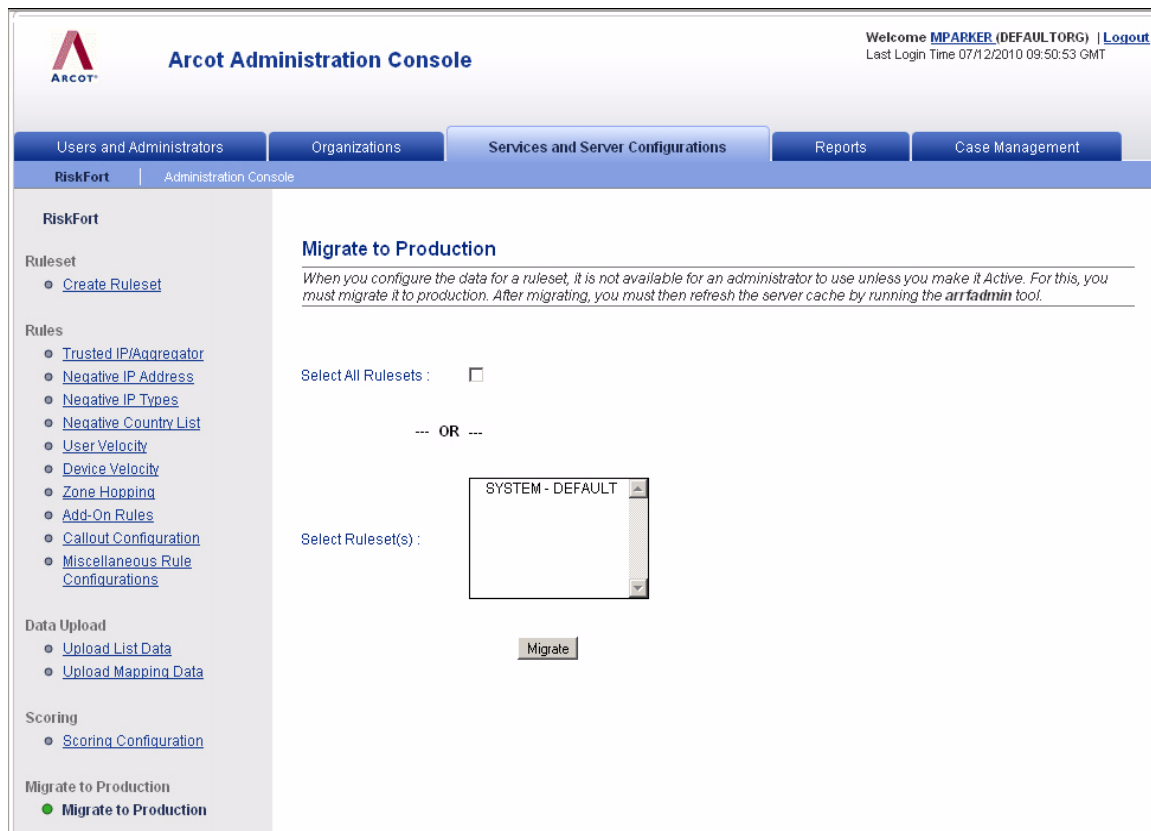
After the Proposed data has been migrated to Active data, if you configure the data again a copy of the Active data is created in Proposed configuration area. Further additions or deletions can be done to the Proposed data until configurations are ready to be migrated to production. All modifications are reflected only in the Proposed data. However, Reports can be viewed as Active or Proposed configurations.



Note: Active data is versioned to keep track of the changes made to the RiskFort configuration data. Every time the Proposed data is migrated to production, unique data versions are created for the new set of Active configuration data.

[Figure 8-2](#) shows the Migrate to Production page that you can use to do so.

Figure 8-2 Migrate to Production Page



To migrate changes from Proposed configuration area to Active data area:

1. Ensure that you are logged in as a GA or as an OA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Migrate to Production** section on the side-bar menu, click the **Migrate to Production** link.

The Migrate to Production page appears, as shown in [Figure 8-2](#).

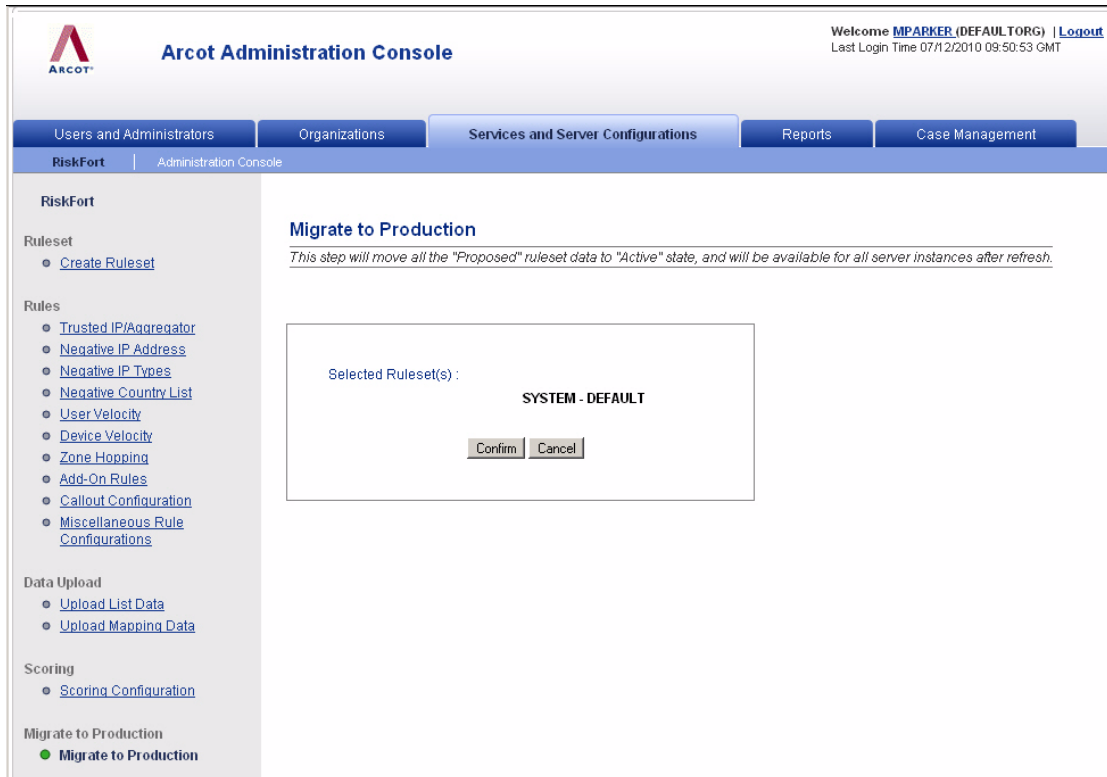
4. On the page, either:
 - Select the **Select All Rulesets** option, if you want to migrate all the changes that you made to all the configured rulesets.

or

- Select a specific ruleset from the **Select Ruleset(s)** list to migrate the changes that you made to this ruleset.
5. Click **Migrate**.

The page to confirm the action is displayed, as shown in [Figure 8-3](#).

Figure 8-3 Migrate to Production: Confirmation Page



6. On the confirmation page, click **Confirm** to start the *migration process*.

Note: Based on the volume of data that you are migrating to production, this might take a few minutes.

After the migration is completed, the "The proposed data has been successfully migrated to Production." message is displayed.

7. Run the **arrfadmin** tool to refresh the RiskFort Server cache as follows:

a. Navigate to the following directory:

- **On Windows:**

```
<install_location>\Arcot Systems\bin\
```

- **On UNIX-Based Platforms:**

```
<install_location>/arcot/bin/
```

b. Run the following command:

arrfadmin -r

Before you use the command, set the **Host** and **Port** values in `riskfortadminclient.ini`. See [“Configuring the Tool for Two-Way SSL Communication with the Server”](#) on page 17-305 for more information.

Chapter 9

Configuring Callouts



Important: All the configurations and tasks discussed in this chapter can be performed by **Global Administrators** to apply the rules globally or by **Organization Administrators** to apply the rules for an organization.

See [Chapter 11, “Managing Organization-Specific RiskFort Configurations”](#) for more information to access the task page for performing the organization-specific configurations:

A *Callout* is a custom component (which can be written in a programming language of your choice) to modify or augment the standard functionality of RiskFort. A Callout, typically, is an external process. As a result, it resides "outside" of the RiskFort Server context and is hosted on a separate HTTPS-based server. Being an external process, you must configure a Callout by using the Administration Console, so that it is invoked when required.

This chapter describes what are the types of Callouts that RiskFort supports and how to configure these Callouts to meet your business requirements. In addition, this chapter also walks you through the deployment, configuration, and use of the Sample Callout that is shipped in the RiskFort package:

- [Understanding Callouts](#)
- [Configuring Callouts](#)
- [Working with the Sample Callout](#)



Note: The administrator performing configuration-related activities *must have* privileges to perform these operations. For more information on the privileges available to administrators at each level, refer to the section, [“Summary of Administrative Privileges” on page 1-10](#).

After you configure a Callout, the changes are not immediately **active** (available to your end users.) You *must* use the **Migrate to Production** link in the side-bar menu of the Administration Console to "move" all **proposed** configuration changes to your production database. See [“Migrating to Production” on page 8-121](#) for steps to migrate to production.

Understanding Callouts

Based on your business requirements, you can write your own custom Evaluation logic and Scoring logic which, if implemented, will run at your application-end, outside of the RiskFort context. These custom Evaluation or Scoring programs are known as **Callouts** that can also be implemented to interact with your application's back-end system.



Note: RiskFort is shipped with a basic Sample Callouts WAR file ([riskfort-2.2.6-sample-callouts.war](#)) that demonstrates how you can write and implement simple Evaluation and Scoring Callouts. See [“Working with the Sample Callout”](#) for more information on deploying and configuring this file.

For example, in addition to tracking the origin of each transaction, a banking institution would also like to assess the risk of regular bank transactions and wire transfers based on the transaction amount. Say, the bank would like to evaluate all transactions more than \$30,000 for risk, irrespective of whether they are regular transactions or wire transfers. In this case, in addition to using RiskFort's Negative Country, Negative IP, Zone Hopping, and Velocity checks, the institution can write an Evaluation Callout (within the scope of their application) to track this behavior.



Note: After Callout is deployed, you *must* enable it by using the Callout Configuration page ([Figure 9-2](#)) for it to take effect.

Callout Implementation



Note: Implementation of Callouts is optional.

If you have implemented a Callout, then RiskFort Server reads all configurations related to the Callout from the database and caches the information on startup. During a transaction:

1. RiskFort Server calls the Callout framework *after* executing all pre-defined and add-on rules (in case of Evaluation Callout) or the standard Scoring Engine (in case of Scoring Callout.)



Note: The Callout framework is a part of RiskFort Server and just like any other RiskFort Evaluation rule, is loaded during the Server startup. It is implemented as a `.dll` or `.so` file.

2. Depending on the type of Callout (**Evaluation** or **Scoring**), the framework collects all the required data from the RiskFort Server and prepares the `HTTP` or `HTTPS` data.



Note: RiskFort supports both one-way and two-way SSL-based connections between the RiskFort Server and your Callout in case of `HTTPS` data.

3. This data is then posted (`HTTP` or `HTTPS`) to the (configured) URL of your Callout.

The Callout framework now waits for a response from your Callout.

If the response from your Evaluation Callout is received within a specified time-out period, then the framework parses the response and sends the result to the RiskFort Server.

If the response is not received within the specified time-out period, then the framework returns `FAILURE` as rule result and empty strings ("") for the modifier and annotation.

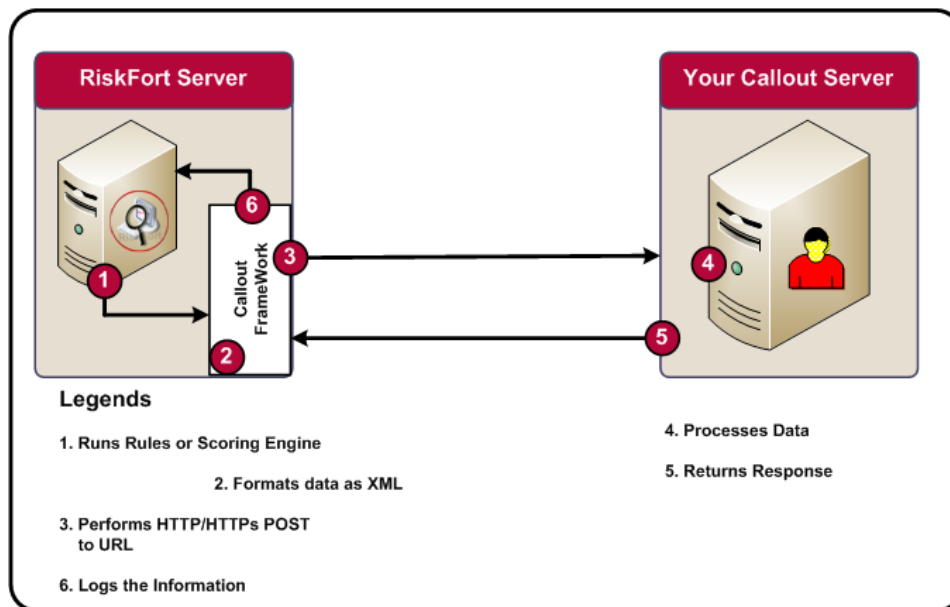


Note: The time-out period can be configured by using the Administration Console.

4. Your Callout processes the data using custom logic.
5. Your Callout then returns an appropriate response to the Callout framework, which forwards the same to RiskFort Server.
6. RiskFort Server logs all the information returned by the framework for reporting and auditing purposes.

Figure 9-1 illustrates the interaction between RiskFort Server, Callout Framework, and your Callout.

Figure 9-1 The Interaction Between a Callout and RiskFort



Note: If you are implementing an Evaluation as well as a Scoring Callout, then you can implement them on your same server or on separate servers.

Types of Callouts

RiskFort supports the following two types of Callouts:

- [Evaluation Callout](#)
- [Scoring Callout](#)

Evaluation Callout

An Evaluation Callout is executed as part of risk evaluation. If an Evaluation Callout is implemented, then:

1. RiskFort executes all Standalone, Add-On, and Combination rules and invokes the Callout framework.
2. The RiskFort Callout framework formats the data in XML format.

3. The RiskFort Callout framework performs an HTTP or HTTPS POST of the following information to your Evaluation Callout:
 - **Context information** (such as User name, IP address, and Device ID) that is passed to each RiskFort Evaluation rule.
 - **Rule results** for each Evaluation rule that was executed.
 - **Additional Inputs**, if any, that are provided by the RiskFort SDK to the RiskFort Server as input data.
4. Your Callout uses the data passed by RiskFort to process its custom logic.
5. Your Callout then returns the following information to RiskFort:
 - **Rule result** in form of **Y** (SUCCESS) or **N** (FAILURE).
 - **Modifier string** with additional information, if any, to be used by the Scoring Callout (if implemented.)



Note: RiskFort Server does not process the modifier string at all. If a Scoring Callout also has been implemented, then RiskFort Server POSTs this data to the Scoring Callout.

- **Annotation string** that contains the reason or the description sent back to RiskFort Server.



Note: This information is used for logging (in the database) for reporting and auditing purposes.

6. RiskFort Server logs the information returned by your Callout.

Scoring Callout

A *Scoring Callout* is executed *after* the standard RiskFort Scoring logic has executed. If a Scoring Callout is implemented, then:

1. RiskFort Server executes the standard Scoring program and invokes the Callout framework.
2. The RiskFort Callout framework formats the data in XML format.
3. The RiskFort Callout framework performs an [HTTP](#) or [HTTPS](#) POST of the following information to your Scoring Callout:
 - **Overall Score** computed by the standard RiskFort built-in Scoring Engine.

- **Rule results** for each Evaluation rule that was executed.
 - **Additional Inputs**, if any, that are provided by the calling application as part of the `evaluateRisk()` API call.
 - **Modifier string** originally returned by the Evaluation Callout.
4. Your Callout uses the data passed by RiskFort to process its custom logic.
 5. Your Callout then returns the following information to RiskFort:
 - **Final Score** in form of an integer in the range [0 – 100].



Note: The score returned by the Scoring Callout always overrides the Score computed by the RiskFort Scoring Engine. If you want to retain the score computed by RiskFort's standard Scoring Engine, then you will need to pass that same Score as the return value in your response.

- **Annotation string** that contains the reason or the description sent back to RiskFort Server. For example, you can put the reason for changing the score in the Annotation field.



Note: This information is used for logging (in the database) for reporting and auditing purposes.

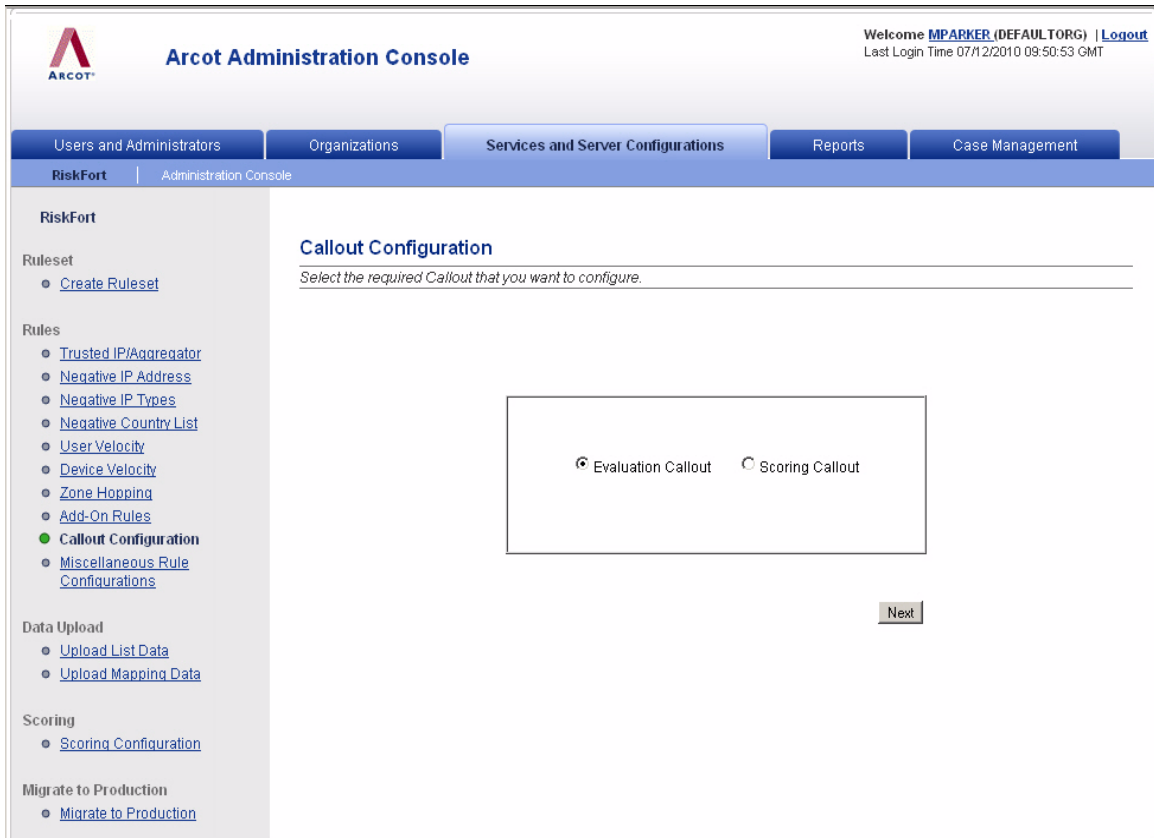
6. RiskFort Server logs the information returned by your Callout.

Configuring Callouts

Use the Callout Configuration page, as shown in [Figure 9-2](#) for:

- [Configuring Evaluation Callout](#)
- [Configuring Scoring Callout](#)

Figure 9-2 Callout Configuration Page



Note: RiskFort is shipped with a basic Sample Callouts WAR file ([riskfort-2.2.6-sample-callouts.war](#)) that demonstrates how you can write and implement Evaluation and Scoring Callouts. See “[Working with the Sample Callout](#)” later in the chapter for more information on deploying and configuring this file.

Configuring Evaluation Callout

To configure an Evaluation Callout, perform the following steps:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.

- Under the **Rules** section on the side-bar menu, click the **Callout Configuration** link.

The Callout Configuration page appears, as shown in [Figure 9-2](#).

- Ensure that the **Evaluation Callout** option is selected and click **Next**.

The Evaluation Callout Configuration page, shown in [Figure 9-3](#), appears.

- From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.

The configuration information for the specified ruleset appears.

- If required, expand the **Advanced Options** section by clicking the **[+]** sign.

- If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is.



Note: You *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The *Update* Evaluation Callout Configuration page is displayed, as shown in [Figure 9-3](#).

Figure 9-3 Evaluation Callout Configuration Page

**Arcot Administration Console**

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

Users and Administrators

Organizations

Services and Server Configurations

Reports

Case Management

RiskFortAdministration Console

RiskFort

Ruleset

- Create Ruleset

Rules

- Trusted IP/Aggregator
- Negative IP Address
- Negative IP Types
- Negative Country List
- User Velocity
- Device Velocity
- Zone Hopping
- Add-On Rules
- Callout Configuration**
- Miscellaneous Rule Configurations

Data Upload

- Upload List Data
- Upload Mapping Data

Scoring

- Scoring Configuration

Migrate to Production

- Migrate to Production

Organization Name:Display Name:Status:

Evaluation Callout Configuration

Specify the settings to deploy your custom Evaluation logic, which will be executed as a part of risk evaluation. The changes that you make on this page will not be effective unless you migrate them to production and refresh the server cache by running the **arradmin** tool.

Update Existing Ruleset
SYSTEM - DEFAULT

Advanced Options

☒ Use Own☐ Refer an Existing Ruleset

☐ Copy from an Existing Ruleset

Ruleset Name --Select--

Callout Elements	Active	Proposed
Update Interval (seconds)	100 milliseconds	1 -
Callout Server Root Certificate	Not Available	Browse
RiskFort Server Certificate and Private Key	Not Available	Certificate: Browse Private Key: Browse
Callout Description	Not Available	

Save

8. In the table, under the **Proposed** column:

Configuring Callouts

September 2010

135

- a. Select the appropriate SSL option for **Server Authentication SSL**.

	Important: If you want to configure, SSL-based communication between RiskFort Server and your Callout, then you must select YES.

- b. Select the appropriate SSL option for **Client Authentication SSL**:

	Note: The client here is your Callout.

- If you want to configure two-way SSL connection between RiskFort Server and your Callout, then you must select **YES** and ensure that the **Server Authentication SSL** is also set to **YES**.
 - If you want to configure one-way SSL connection between RiskFort Server and your Callout, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is also set to **YES**.
 - If you do not want to configure any SSL-based connection, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is also set to **NO**.
- c. Specify the URL at which the Callout is available against **Callout URL**.
- If **Server Authentication SSL** is set to **YES** or **Client Authentication SSL** is set to **YES**, then the URL of Evaluation Callout *must* begin with <https://>.
 - If both **Server Authentication SSL** is set to **NO** and **Client Authentication SSL** is set to **NO**, then the URL of Evaluation Callout *must* begin with <http://>.
- d. Specify the value of **Connection Timeout** in seconds.
- Connection Timeout* indicates the time in which connection between RiskFort Server and your Callout will expire.
- e. Specify the value of **Read Timeout** in seconds.
- Read Timeout* indicates the time in which RiskFort Server expects a response back from your Callout.

- f. Click **Browse** to navigate to the location where the **Callout Server Root Certificate** is located.

	Note: That: - If Server Authentication SSL is set to YES <i>or</i> Client Authentication SSL is set to YES, then you <i>must</i> specify the Callout Server Root Certificate. - Callout Server Root Certificate <i>must</i> be in PEM (Base64-encoded) format.

- g. Click **Browse** to navigate to the location where the **RiskFort Server Certificate and Private Key** are located.

	Note: That: - If Client Authentication SSL is set to YES, then you <i>must</i> specify the Callout Server Root Certificate and RiskFort Server Certificate and Private Key. - RiskFort Server Certificate and Private Key <i>must</i> be in PEM (Base64-encoded) format.

- h. Specify useful details about the Callout against **Callout Description**.
9. Click **Save** to save the changes that you just made.
- The changes are yet not active, and not available to your end users.
10. To make the changes active, you must migrate them to production.
- Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Configuring Scoring Callout

To configure a Scoring Callout, perform the following steps:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Under the **Rules** section on the side-bar menu, click the **Callout Configuration** link.

The Callout Configuration page (Figure 9-2) appears.

4. Select the **Scoring Callout** option and click **Next**.

The Scoring Callout Configuration page appears.

5. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
6. Expand the **Advanced Options** section (Figure 9-4) by clicking the **[+]** sign.
7. If required, in the **Advanced Options** section select *one* of the following options:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.

Note that the changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

The *Update* Scoring Callout Configuration page is displayed, as shown in Figure 9-4.

Figure 9-4 Scoring Callout Configuration Page


Arcot Administration Console

Welcome **MPARKER (DEFAULT.TORG)** | [Logout](#)
Last Login Time 07/12/2010 09:50:53 GMT

[Users and Administrators](#)
[Organizations](#)
[Services and Server Configurations](#)
[Reports](#)
[Case Management](#)

[RiskFort](#) | [Administration Console](#)

RiskFort

Ruleset

- [Create Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)**
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Migrate to Production

- [Migrate to Production](#)

Organization Name: _____ **Display Name:** _____ **Status:** _____

Scoring Callout Configuration

Specify the settings to deploy your custom Scoring logic, which will be executed after RiskFort's Scoring logic. The changes that you make on this page will not be effective unless you migrate them to production and refresh the server cache by running the `arradmin` tool.

Update Existing Ruleset
SYSTEM - DEFAULT

[Advanced Options](#)

☒ Use Own ☐ Refer an Existing Ruleset
☐ Copy from an Existing Ruleset
Ruleset Name: --Select--

☒ Use Own ☐ Refer an Existing Ruleset
☐ Copy from an Existing Ruleset
Ruleset Name: --Select--

Server Authentication SSL	NO	☒ YES ☒ NO
Client Authentication SSL	NO	☒ YES ☒ NO
Callout URL	Not Available	
Connection Timeout (Seconds)	Not Available	
Read Timeout (Seconds)	Not Available	
Callout Server Root Certificate	Not Available	Browse...
RiskFort Server Certificate and Private Key	Not Available	Certificate: Browse...
		Private Key: Browse...
Callout Description	Not Available	

Save

8. In the table, under the **Proposed** column:

- a. Select the appropriate SSL option for **Server Authentication SSL**.

	Important: If you want to configure, SSL-based communication between RiskFort Server and your Callout, then you must select YES .

- b. Select the appropriate SSL option for Client Authentication SSL:

	Note: The client here is your Callout.

- If you want to configure two-way SSL connection between RiskFort Server and your Callout, then you must select **YES** and ensure that the **Server Authentication SSL** is also set to **YES**.
 - If you want to configure one-way SSL connection between RiskFort Server and your Callout, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is also set to **YES**.
 - If you do not want to configure any SSL-based connection, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is also set to **NO**.
- c. Specify the URL at which the Callout is available against **Callout URL**.
- If **Server Authentication SSL** is set to **YES** or **Client Authentication SSL** is set to **YES**, then the URL of Evaluation Callout *must* begin with <https://>.
 - If both **Server Authentication SSL** is set to **NO** and **Client Authentication SSL** is set to **NO**, then the URL of Evaluation Callout *must* begin with <http://>.
- d. Specify the value of **Connection Timeout** in seconds.
- Connection Timeout* indicates the time in which connection between RiskFort Server and your Callout will expire.
- e. Specify the value of **Read Timeout** in seconds.
- Read Timeout* indicates the time in which RiskFort Server expects a response back from your Callout.
- f. Click **Browse** to navigate to the location where the **Callout Server Root Certificate** is located.

	Note: That: - If Server Authentication SSL is set to YES <i>or</i> Client Authentication SSL is set to YES, then you <i>must</i> specify the Callout Server Root Certificate. - Callout Server Root Certificate <i>must</i> be in PEM (Base64-encoded) format.

- g. Click **Browse** to navigate to the location where the **RiskFort Server Certificate and Private Key** are located.

	Note: That: - If Client Authentication SSL is set to YES, then you <i>must</i> specify the Callout Server Root Certificate and RiskFort Server Certificate and Private Key. - RiskFort Server Certificate and Private Key <i>must</i> be in PEM (Base64-encoded) format.

- h. Specify useful details about the Callout against **Callout Description**.
9. Click **Save** to save the changes that you just made.
- The changes are yet not active, and not available to your end users.
10. To make the changes active, you must migrate them to production.
- Refer to [“Migrating to Production” on page 8-121](#) for instructions to do so.

Working with the Sample Callout

RiskFort 2.2.6 is shipped with a basic and non-GUI Sample Callouts WAR file ([riskfort-2.2.6-sample-callouts.war](#)) that demonstrates:

- The basic operations (invocation and post-processing) of RiskFort Server from your custom program.

- The integration of your Callout with RiskFort.

This Sample Callouts WAR file is automatically installed as a part of **Complete** installation of RiskFort. As a part of **Custom** installation, you *must* select to install the **RiskFort Server** component to access this WAR file.



Important: Sample Callouts *must* be deployed on the same application server where RiskFort Server is installed.

This section covers:

- [Deploying Sample Callouts](#)
- [Configuring RiskFort Server to Communicate With Sample Callouts](#)
- [Using the Sample Callout](#)

Deploying Sample Callouts

This section walks you through the steps for deploying Sample Callouts:

- [On Windows](#)
- [On UNIX-Based Platforms](#)

On Windows

To deploy the Sample Callouts shipped with RiskFort on Windows on your application server:

1. Navigate to **Settings -> Control Panel -> Administrative Tools -> Services**.
2. Stop the application server services.
3. Deploy the `riskfort-2.2.6-sample-callouts.war` file on *from* the following location:

```
<install_location>\Arcot Systems\samples\java\
```



Note: Although you will also see `riskfort-2.2.6-sample-callouts.war` in the package, it is recommended that you deploy the Sample Application WAR file from the preceding location.

4. Navigate to **Settings -> Control Panel -> Administrative Tools -> Services**.
5. Restart the application server services.

On UNIX-Based Platforms

To deploy the Sample Callouts shipped with RiskFort on UNIX-based platforms on your application server:

1. Stop the application server services.
2. Deploy the `riskfort-2.2.6-sample-callout.war` file *from* the following location:

```
<install_location>/arcot/samples/java/
```



Note: Although you will also see `riskfort-2.2.6-sample-callout.war` in the package, it is recommended that you deploy the Sample Application WAR file from the preceding location.

3. Restart the application server services.

Configuring RiskFort Server to Communicate With Sample Callouts

To configure the Sample Callouts, perform the following steps:

1. Perform the tasks listed from [Step 1](#) through [Step 7](#) to display the **Evaluation Callout Configuration** table.
2. Under the **Proposed** column of the table:
 - a. Select **NO** for **Server Authentication SSL**.
 - b. Select **NO** for Client Authentication SSL:



Note: The client here is the Sample Callout.

- c. Specify the following against the **Callout URL** option:

<http://<host>:<port>/riskfort-2.2.6-sample-callouts/SampleEvalCalloutServlet>

Here, `<host>` refers to the host name or IP address of the server where your Callouts WAR is deployed and `<port>` refers to the port on which this server is available.

- d. Specify the value of **Connection Timeout** in seconds. The default value is 30 seconds.

- e. Specify the value of **Read Timeout** in seconds. The default value is 30 seconds.
 - f. Specify useful details about the Callout against **Callout Description**.
 - g. Click **Save** to save the changes that you just made.
3. Perform the tasks listed from [Step 1](#) through [Step 6](#) to display the **Scoring Callout Configuration** table.
 4. Under the **Proposed** column of the table:
 - a. Select **NO** for **Server Authentication SSL**.
 - b. Select **NO** for **Client Authentication SSL**:



Note: The client here is the Sample Callout.

- c. Specify the following against the **Callout URL** option:
<http://<host>:<port>/riskfort-2.2.6-sample-callouts/SampleScoringCalloutServlet>
 Here, [<host>](#) refers to the host name or IP address of the server where your Callouts WAR is deployed and [<port>](#) refers to the port on which this server is available.
 - d. Specify the value of **Connection Timeout** in seconds. The default value is 30 seconds.
 - e. Specify the value of **Read Timeout** in seconds. The default value is 30 seconds.
 - f. Specify useful details about the Callout against **Callout Description**.
 - g. Click **Save** to save the changes that you just made.
5. Under the **Scoring** section on the side-bar menu, click the **Scoring Configuration** link.
 The Scoring Configuration page appears.
 6. Scroll to the end of the table to **Evaluation Callout** and **Scoring Callout**, and make the following changes under the **PROPOSED** column for *each*:
 - a. Select **Enabled Execution**.
 - b. Select **Enabled Scoring**.
 - c. Specify the **Risk Score**.
 - d. Click **Save** to save the changes.

All the changes that you made until now are yet not active, and not available to your end users.

7. To make the changes active, you must migrate them to production.

Refer to “[Migrating to Production](#)” on page 8-121 for instructions to do so.

Using the Sample Callout

Unlike the Sample Application shipped with RiskFort, Sample Callout does not have a user interface that you can access using the browser. It just demonstrates how data can be posted to the respective Callout (Evaluation or Scoring) and how to send response back to RiskFort Server. However, you can use the Sample Callout in collaboration with the Sample Application to see how it affects the default risk evaluation and scoring behavior. To do so:

1. Start the Sample Application in a Web browser window. The default URL for Sample Application is:

<http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp>

The RiskFort Sample Application page appears.

2. Create a new user by clicking **Create User**.
3. After the user has been created, return to the RiskFort Sample Application page by clicking **Main Page**.
4. Click **Evaluate Risk** to perform risk evaluation for the new user you just created.

By default, Sample Application generates the Risk Score of 65 and Risk Advice as INCREASEAUTH. However after deploying and configuring the Sample Callout, you will see Risk Score of 85 and Risk Advice as DENY.

Chapter 10

Managing Organizations



Note: Most of the tasks in this chapter can be performed by a Global Administrator (GA) or an Organization Administrator (OA), if they have the required scope to the organization.

In the Arcot Administration Console, an *organization* can either map to a complete enterprise (or a company) or a specific division, department, or other entities within the enterprise. The organization structure provided by the Administration Console is flat. In other words, organizational hierarchy (in form of parent and child organizations) is *not* supported, and all organizations are created at the same level as the Default Organization. (See [“Specifying Global Settings for Organizations” on page 2-29](#) for more information on Default Organization.)

The larger the enterprise, the more complex its organization structure. As a result, management of organizations is a critical part of administration. The organization management operations supported by RiskFort include:

- [Creating and Activating Organizations](#)
- [Searching for Organizations](#)
- [Updating Organization Information](#)
- [Disabling Organizations](#)
- [Enabling Organizations](#)
- [Activating Organizations in Initial State](#)
- [Deleting Organizations](#)



Note: In addition to the preceding list of tasks related to organization management, OAs can also manage organization-specific configurations. See [Chapter 11, “Managing Organization-Specific RiskFort Configurations”](#) for more information related to this.

Creating and Activating Organizations

You can create an organization and store its data either in the RiskFort repository or in your existing LDAP-based directory server implementations, such as Microsoft Active Directory and Sun ONE Directory Server.



Note: In case of a small deployment, you can rename the Default Organization, instead of creating a new organization.

Based on your implementation, this section guides you through the steps for:

- [Creating Organizations in Arcot Repository](#)
- [Creating Organization in LDAP Repository](#)

Privileges Required

To be able to create and activate an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can create and activate all organizations. GAs can create and activate all organizations in their scope.

Creating Organizations in Arcot Repository

To create an organization in the Arcot repository:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Create Organization** link to display the Create Organization page ([Figure 10-1.](#))

Figure 10-1 Create Organization Page

Arcot Administration Console

Welcome **MPARKER (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:00 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

Manage Organizations

Manage Organizations

- Create Organization**
- [Search Organization](#)

Create Organization

In addition to the basic organization information, specify the authentication mechanism to be used for logging in administrators and the location of the repository where the user data is available.

Organization Information

Organization Name: *

Display Name: *

Description:

Administrator Authentication Mechanism: *

User Data Location

Repository Type: *

- Enter the details of the organization, as discussed in [Table 10-1](#).

Table 10-1. Create Organization Fields

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. NOTE: You have to specify this value to log in to this organization, <i>not</i> the Display Name of the organization.
Display Name	Enter the descriptive name for the organization. NOTE: This name appears on all other Administration Console pages and reports.

Table 10-1. Create Organization Fields

Field	Description
Description	Provide a description for the administrators who will manage this organization. NOTE: You can provide additional details for later reference for the organization by using this field.
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators belonging to this organization. Administration Console supports the following two types of authentication mechanisms: • Basic User Password This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators log in to the console by specifying their ID and password. • WebFort User Password This is the WebFort user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by WebFort Server. To use this mechanism, you must have Arcot WebFort 6.0 installed and configured for this option to work. Refer to the Arcot WebFort 6.0 Installation and Deployment Guide for detailed information on how to deploy WebFort.
User Data Location	
Repository Type	Select Arcot Database . By specifying this option, the user and administrator details for the new organization will be stored in the RDBMS repository supported by WebFort.

5. Click **Create** to create the new organization.

The Add Administrators page ([Figure 10-2](#)) appears.



Note: This page is *not* displayed, if all the administrators currently present in the system have scope to manage all organizations.

Figure 10-2 Add Administrators

Arcot Administration Console

Welcome **MPARKER(DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:00 GMT

Users and Administrators | **Organizations** | **Services and Server Configurations** | **Reports** | **Case Management**

Manage Organizations

Manage Organizations

- [Create Organization](#)
- [Search Organization](#)

Add Administrators

Add the administrators (from the list of Available Administrators) who will manage this organization.

Administrators for this Organization

Available Administrators

- FANTONY(DEFAULTORG)
- JHUME(DEFAULTORG)
- LWARD(DEFAULTORG)
- PRUSH(DEFAULTORG)
- RGRAHAM(DEFAULTORG)

Managing Administrators

> >> < <<

[Next](#)

- From the **Available Administrators** list, select the administrators who will manage the organization and click the > button to add the administrator to the **Managing Administrators** list.

The **Available Administrators** list displays all the administrators who can manage the new organization.



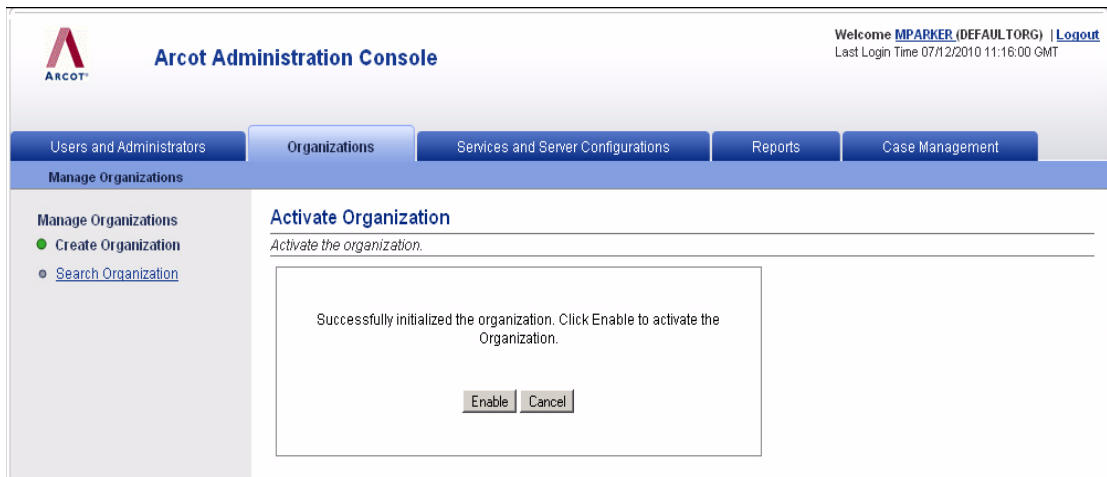
Note: If some administrators have scope to manage all organizations in the system, then you will not see the corresponding entries for those administrators in this list.

The **Managing Administrators** list displays the administrators that you have selected to manage this organization.

- Click **Next** to proceed.

The Activate Organization page (Figure 10-3) appears.

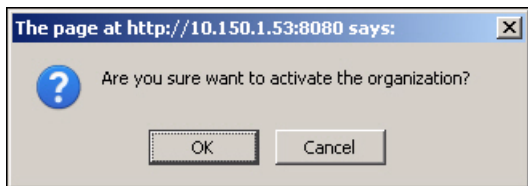
Figure 10-3 Activate Organization



8. Click **Enable** to activate the new organization.

The message box shown in [Figure 10-4](#) appears.

Figure 10-4 Activate Organization: Message



9. Click **OK** to complete the process.
10. Refresh *all* deployed RiskFort Server instances. See [“Refreshing or Shutting Down a Server Instance”](#) on page 4-52 for instructions on how to do this.

Creating Organization in LDAP Repository

To support LDAP user directories, you must create an organization in Arcot repository and then map the Arcot attributes with the LDAP attributes. To do so:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.

- Under the **Manage Organizations** section, click the **Create Organization** link to display the Create Organization page (Table 10-1.)
- Enter the details of the organization, as discussed in Table 10-2.

Table 10-2. Create Organization Fields in LDAP Repository

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. NOTE: You can use the Administration Console to log in to this organization, by specifying this value, <i>not</i> the Display Name of the organization.
Display Name	Enter the descriptive name for the organization. NOTE: This name appears on all other Administration Console pages and reports.
Description	Provide a description for the administrators who will manage this organization. NOTE: You can provide additional details for later reference for the organization by using this field.
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators belonging to this organization. Administration Console supports the following two types of authentication mechanisms: • Basic User Password This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators log in to the console by specifying their ID and plain text password. • WebFort User Password This is the WebFort user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by WebFort Server. To use this mechanism, you must have Arcot WebFort 6.0 installed and configured for this option to work. Refer to the Arcot WebFort 6.0 Installation and Deployment Guide for detailed information on how to deploy WebFort.
User Data Location	
Repository Type	Select Enterprise LDAP . By specifying this option, the user and administrator details for the new organization will be stored in the LDAP repository that you will specify on the next page.

- Click **Create** to create the new organization.

The Create Organization page (Figure 10-5) to collect the LDAP repository details appears.

Figure 10-5 Create Organization: Enterprise LDAP Details

The screenshot shows the Arcot Administration Console interface. The top navigation bar includes 'Users and Administrators', 'Organizations' (selected), 'Services and Server Configurations', 'Reports', and 'Case Management'. The left sidebar shows 'Manage Organizations' with 'Create Organization' selected. The main content area is titled 'Create Organization' and contains a sub-section 'Enterprise LDAP Details' with the following fields:

- Host Name: *
- Port Number: *
- Schema Name: *
- Base Distinguished Name: *
- Connection Type: * (Dropdown menu showing 'TCP')
- Login Name: *
- Login Password: *
- Server Trusted Root Certificate: (Text input) Browse...
- Client Key Store: (Text input) Browse...
- Client Key Store Password: *

A 'Next' button is located at the bottom of the form.

6. Enter the details, discussed in [Table 10-3](#), to connect to the LDAP repository.

Table 10-3. LDAP Repository Details

Field	Description
Host Name	Enter the host name of the system where the LDAP repository is available.
Port Number	Enter the port number on which the LDAP repository service is listening.
Schema Name	Specify the LDAP schema used by the LDAP repository. This schema specifies the types of objects that an LDAP repository can contain, and specifies the mandatory and optional attributes of each object type. Typically, the schema name for Active Directory is <code>user</code> and for SunOne Directory it is <code>inteorgperson</code> .

Table 10-3. LDAP Repository Details

Field	Description
Base Distinguished Name	Enter the base Distinguished Name of the LDAP repository. This value indicates the starting node in the LDAP hierarchy to search in the LDAP repository. For example, to search or retrieve a user with a DN of <code>cn=rob laurie, ou=sunnyvale, o=arcot, c=us</code>, you must specify the base DN as the following: • <code>ou=sunnyvale, o=arcot, c=us</code> Note: Typically, this field is case sensitive and searches all sub-nodes under the provided base DN.
Connection Type	Select the type of connection that you want to use between the Administration Console and the LDAP repository. Supported types are: • TCP • One-way SSL • Two-way SSL
Login Name	Enter the complete distinguished name of the LDAP repository user who has the privilege to log into repository sever and manage the Base Distinguished Name. For example, <code>uid=gt,dc=arcot,dc=com</code>
Login Password	Enter the password of the user provided in the Login Name .
Server Trusted Root Certificate	Enter the path for the trusted root certificate who issued the SSL certificate to the LDAP server by using the Browse button, if the required SSL option is selected.
Client Key Store Path	Enter the path for the key store that contains the client certificate and the corresponding key by using the Browse button, if the required SSL option is selected. Note: You must upload either PKCS#12 or JKS key store type.
Client Key Store Password	Enter the password for the client key store, if the required SSL option is selected.

7. Click **Next** to proceed.

The page ([Figure 10-6](#)) to map the repository attributes appears.

Figure 10-6 Create Organization: Repository Attribute Mapping

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo, the title 'Arcot Administration Console', and a user welcome message: 'Welcome MPARKER (DEFAULTORG) | Logout' with a last login time of '07/05/2010 05:21:50 GMT'. Below the header is a navigation bar with tabs: 'Users and Administrators', 'Organizations' (selected), 'Services and Server Configurations', 'Reports', and 'Case Management'. Under the 'Organizations' tab, there's a sub-tab 'Manage Organizations'. On the left sidebar, under 'Manage Organizations', there are two links: 'Create Organization' (highlighted with a green dot) and 'Search Organization'. The main content area is titled 'Create Organization' and contains a note: 'Specify the LDAP Attribute Mapping details for the organization. Note: The USERNAME Mapping is mandatory. You will not be able to change these mappings after the organization has been activated.' Below this note is a section titled 'Repository Attribute Mapping'. This section contains three lists of attributes: 'Arcot Database Attributes' (DATECREATED, DATEMODIFIED, EMAILADDR, FNAME, LNAME, MNAME, PAM, STATUS), 'Enterprise LDAP Attributes' (audio, businessCategory, carLicense, cn, departmentNumber, description, destinationIndicator, displayName), and 'Mapped Attributes' (empty). There are 'Map', 'UnMap', and 'Reset' buttons between the Enterprise LDAP Attributes and Mapped Attributes lists. A 'Next' button is at the bottom of the mapping section.

8. On this page:
 - a. Select an attribute from the **Arcot Database Attributes** list, then select the appropriate attribute from the **Enterprise LDAP Attributes** list that needs to be mapped with the Arcot attribute, and click **Map**.

	Important: Mapping of the <code>UserName</code> attribute is compulsory. If you are using Active Directory, then map <code>UserName</code> to <code>cn</code>. If you are using SunOne Directory, then map <code>UserName</code> to <code>uid</code>.

- b. Repeat the process to map multiple attributes, until you finish mapping all the required attributes.



Note: You do not need to map all the attributes in the **Arcot Database Attributes** list. You only need to map the attributes that you will use.

The attributes that you have mapped will be moved to the **Mapped Attributes** list.

If required, you can unmap the attributes. If you want to unmap a single attribute at a time, then select the attribute and click **Unmap**. However, if you want to clear the **Mapped Attribute** list, then click **Reset** to unmap all the mapped attributes.

9. Click **Next** to proceed.

The Add Administrators page ([Figure 10-2](#)) appears.



Note: This page is *not* displayed, if all the administrators currently present in the system have scope to manage all organizations.

10. From the **Available Administrators** list, select the administrators who will manage the organization and click the > button to add the administrator to the **Managing Administrators** list.



Note: Assigning organization to administrators can be done at any time by updating the scope of existing administrators or by creating new administrators to manage the organization.

The **Available Administrators** list displays all the administrators who can manage the new organization.



Note: If some administrators have scope to manage all organizations in the system, then you will not see the corresponding entries for those administrators in this list.

The **Managing Administrators** list displays the administrators that you have selected to manage this organization.

11. Click **Next** to proceed.

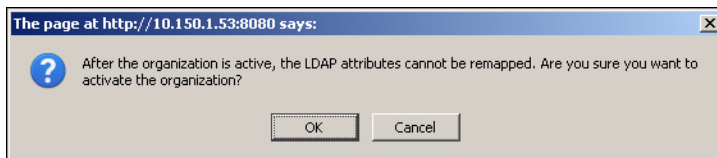
The Activate Organization page (Figure 10-3) appears.

	Note: Mapping details <i>cannot</i> be changed or updated after the organization is activated.

12. Click **Enable** to activate the new organization.

The warning message shown in Figure 10-7 appears.

Figure 10-7 Activate LDAP-Based Organization



13. Click **OK** to complete the process.

Searching for Organizations

Privileges Required

As long as you do not need to update, activate, or deactivate an organization, you do not need privileges to search. However, you *must* have the scope over the organizations that you are searching. For example, an OA can search for a target organization *if* that organization is in their purview.

Searching Organizations

You can search for organizations by their name and status. To search for one or more organizations:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.

- Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 10-8.)

Figure 10-8 Search Organization Page

The screenshot shows the Arcot Administration Console interface. At the top, there's a header with the Arcot logo, the title 'Arcot Administration Console', and a user welcome message 'Welcome PLAUPIE (DEFAULTORG) | Logout' with the last login time '07/12/2010 11:16:24 GMT'. Below the header is a navigation bar with tabs: 'Users and Administrators', 'Organizations' (selected), 'Reports', and 'Case Management'. Under the 'Organizations' tab, there's a sub-section 'Manage Organizations' with a sidebar containing 'Manage Organizations' and 'Search Organization' (selected). The main content area is titled 'Search Organization' and contains a search form. The form has a text input field for 'Organization' and four checkboxes for 'Initial', 'Active', 'Inactive', and 'Deleted'. The 'Active' checkbox is checked. A 'Search' button is located to the right of the checkboxes. Below the form, there's a placeholder text: 'Enter the (full or partial) Display Name of the organization that you want to search.'

- Enter the partial or complete information of the required organization. You can select the following options to broaden your search:



Note: In the **Organization** field, you must enter the partial or complete display name of the organization and *not* the actual organization name.

- **Initial** (to display the organizations that have been created but have not been activated yet.)
- **Active** (to display the organizations that have been created and have been activated.)
- **Inactive** (to display the organizations that have been disabled.)
- **Deleted** (to display the organizations that have been deleted.)

- Click **Search** to display the page (similar to [Figure 10-9](#)), with all the matches for the specified criteria.

Figure 10-9 Search Organization Page: Result

Welcome [PLAUBIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Arcot Administration Console

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations

- Search Organization

Search Organization

Click the Organization Name link to view or edit the details of the selected organization. To enable, disable, or delete multiple organizations, select the required organizations and click the applicable button.
Tip: You can also reorder the list of organizations by clicking the Organization column heading.

Organization	Initial	Active	Inactive	Deleted
	☐	☒	☐	☐

Select Organizations to Modify

☐	Organization	Display Name	Description	Status
☐	HSBC	HSBC		Active
☐	DEFAULTORG	DEFAULT ORGANIZATION	This is the initial default Organization.	Active
☐	SAFE BANK	Safe Bank		Active

Updating Organization Information

By using the Administration Console, you can update the following information for an organization:

- Organization information** that includes organization display name, description, and status, and the administrators that manage the organization (“[Updating the Organization Information](#)”)
- RiskFort-specific configurations** for the organization that include credential profiles, authentication policies, extensible configurations, and the assigned default configurations (“[Updating RiskFort-Specific Configurations](#)”)

Privileges Required

To be able to update an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can update all organizations. GAs and OAs can update the information for all organizations in their scope.

Updating the Organization Information

To update the basic organization information:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 10-8.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

A list of organizations matching the search criteria (similar to Figure 10-9) appears.

5. Under the **Organization** column, click the `<ORGANIZATION_NAME>` link for the required organization.

The Organization Information page (similar to [Figure 10-10](#)) appears.

Figure 10-10 Organization Information Page

Arcot Administration Console

Welcome [RLAURIE](#) (DEFAULTORG) | [Logout](#)
Last Login Time

[Users and Administrators](#) | [Organizations](#) | [Reports](#) | [Case Management](#)

Manage Organizations

Manage Organizations
● [Search Organization](#)

Basic Organization Information
● [Organization Details](#)
● [Basic Authentication Policy](#)

Organization Name: DEFAULTORG Display Name: DEFAULT ORGANIZATION Status: Active

[Basic Organization Information](#) | [RiskFort Configuration](#)

Organization Information
Edit the required fields and click Next to save the changes.

Organization Details

Organization Name: DEFAULTORG
Display Name:
Description:
Administrator Authentication Mechanism: Basic User Password
Date Created: 07/02/2010 05:02:51 GMT
Last Modified: 07/02/2010 05:10:12 GMT
Default Organization: Yes

[Next](#)

6. Edit the required fields (**Display Name** and **Description**) in the **Organization Details** section.
7. Click **Next** to proceed with additional configurations:

- If the organization was created **in the Arcot Repository** and if the administrators in the organization have scope to manage all organizations in the system, then the Update Administrators page (similar to [Figure 10-2](#)) appears.

On this page, update the administrators who will manage the organization and click **Update** to save the changes and complete the process.

- If the organization was created **in the LDAP repository**, then Edit Organization page ([Figure 10-5](#)) appears:
 - i. Use the information in [Table 10-3](#) to update the fields, as required, and click **Next** to display the page to edit the Repository Attribute Mappings ([Figure 10-6](#)).

- ii. You *cannot* edit the mappings that are created when you created the organization. Click **Update** to display the Update Administrators page (Figure 10-6).
- iii. On the Update Administrators page, update the administrators who will manage the organization and click **Update** to save the changes and complete the process.

Updating RiskFort-Specific Configurations

To update the RiskFort configurations of an organization:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 10-8.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button to display a list (similar to Figure 10-9) of organizations matching the search criteria.
5. Under the **Organization** column, click the <ORGANIZATION_NAME> link for the required organization to display the Organization Information page (similar to Figure 10-10) appears.
6. Activate the **RiskFort Configuration** tab to display the links for RiskFort configurations in the task panel.
7. Refer to Chapter 11, “Managing Organization-Specific RiskFort Configurations” for detailed information on these configurations.

Disabling Organizations

When you want to prevent all administrators of an organization from logging in to the Administration Console and end users of the organization from authenticating to your application by using RiskFort mechanisms, you disable the organization.

Privileges Required

To be able to disable an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can disable all organizations. GAs and OAs can disable all organizations in their scope.

Disabling Organizations

To disable one or more organizations:

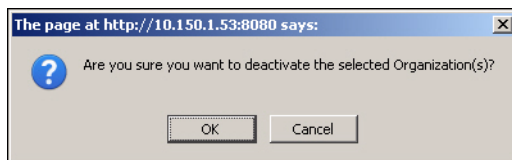
1. Ensure that you are logged in with the required privileges and scope to disable the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 10-8.)
4. Enter the complete or partial information of the organization you want to search and click **Search**.

A list of organizations matching the search criteria (similar to Figure 10-9) appears.

5. Select one or more organizations that you want to disable.
6. Click **Deactivate** to disable the selected organizations.

The message box shown in Figure 10-11 appears.

Figure 10-11 Deactivate Organization: Message



7. Click **OK** to confirm the deactivation.

Enabling Organizations

You might need to re-enable a deactivated organization. In this case, you must select the **Inactive** option while specifying the search criteria on the Search Organization page.

Privileges Required

To be able to enable an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can enable all organizations. GAs and OAs can enable all organizations in their scope.

Enabling Organizations

To enable a deactivated organization:

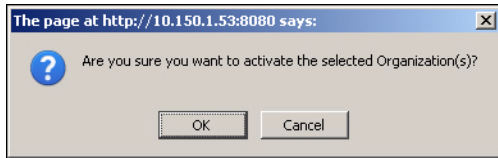
1. Ensure that you are logged in with the required privileges and scope to enable the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 10-8.)
4. Enter the complete or partial information of the organization you want to search and click **Search**.

A list of organizations matching the search criteria (similar to Figure 10-9) appears.

5. Select one or more organizations that you want to enable again.
6. Click **Activate** to enable the selected organizations.

The message box shown in Figure 10-12 appears.

Figure 10-12 Activate Organization: Message



7. Click **OK** to confirm the activation.

Activating Organizations in Initial State

Sometimes you might start creating an organization, but not activate it. For example, you might specify the **Organization Information** and **User Data Location** on the Create Organization page, but not specify the details of the LDAP repository or the administrators who will manage the organization. In such cases, the organization is created, but is not active and is not typically visible in searches (unless you search by selecting the **Initial** option).

Such organizations remain in the Initial state in the system, unless you activate them. If later, you try to create a new organization with same details as an organization in Initial state, the system does not allow you to, because the organization exists.

Privileges Required

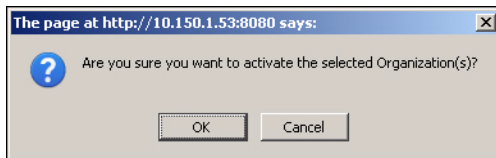
To be able to activate an organization in Initial state, you must ensure that you have the appropriate privileges and scope to do so. MA can activate all organizations. GAs and OAs can activate all organizations in their scope.

Activating Organizations in Initial State

To activate an organization that is in the **Initial** state:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page ([Figure 10-8](#).)
4. Enter the partial or complete information of the required organization and select the **Initial** option.
5. Click **Search** to display the page (similar to [Figure 10-9](#)), with all the matches for the specified criteria.
6. Select the organizations that you want to activate.
7. Click **Activate** to enable the selected organizations. The message box shown in [Figure 10-13](#) appears.

Figure 10-13 Activate Organization: Message



8. Click **OK** to confirm the activation.

Deleting Organizations

After an organization is deleted, the administrators associated with the organization can no longer log into it by using the Administration Console and the end users who belong to this organization cannot authenticate. However, the information related to the organization is still maintained in the system. The administrator who has scope on the deleted organization can read the organization details.

Privileges Required

To be able to delete an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can delete all organizations. GAs and OAs can delete all organizations in their scope.

Deleting Organizations

To delete an organization:

1. Ensure that you are logged in with the required privileges and scope to delete the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 10-8.)
4. Enter the complete or partial information of the organization you want to search and click **Search**.

A list of organizations matching the search criteria (similar to Figure 10-14) appears.

Figure 10-14Deleting Organization

Welcome **PLAURIE (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Arcot Administration Console

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations
● **Search Organization**

Search Organization

*Click the Organization Name link to view or edit the details of the selected organization. To enable, disable, or delete multiple organizations, select the required organizations and click the applicable button.
Tip: You can also reorder the list of organizations by clicking the Organization column heading.*

Organization	Initial	Active	Inactive	Deleted
	☐	☒	☐	☐

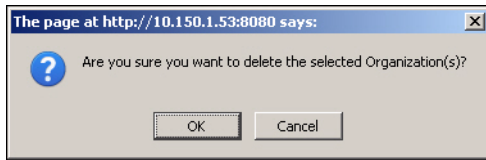
Select Organizations to Modify

	Organization	Display Name	Description	Status
☒	HSBC	HSBC		Active
☒	DEFAULTORG	DEFAULT ORGANIZATION	This is the initial default Organization.	Active
☐	SAFEBANK	Safe Bank		Active

5. Select one or more organizations that you want to delete, and click **Delete**.

The message box shown in [Figure 10-15](#) appears.

Figure 10-15Deleting Organization: Message



6. Click **OK** to confirm the activation.

Chapter 11

Managing Organization-Specific RiskFort Configurations



Note: To be able to manage the configurations of an organization, you (**Organization Administrator**) must ensure that you have the appropriate privileges and scope to do so.

A **Master Administrator** *cannot* manage any organization-specific configurations. GAs and OAs can manage the configurations for all organizations in their scope.

Although you can refer to or create a copy of the "templated" rule settings configured by the Global Administrators (GAs) (as discussed in [Chapter 7, “Managing Global Rule Configurations”](#)), you might want to override them to meet the specific business requirements of the organizations in your purview.

When you set rule configurations at the level of an organization, the changes are restricted to the specific organization where they were set. Also, the changes you make to the configurations are *not* applied automatically. You need to refresh all server instances to apply these configuration changes.

As an OA, if you have the scope on the given organizations, then you can perform the following tasks:

- [Accessing Organization-Specific RiskFort Configurations](#)
- [Creating Rulesets](#)
- [Assigning Rulesets](#)
- [Using Global Configurations](#)
- [Configuring RiskFort for An Organization](#)

Accessing Organization-Specific RiskFort Configurations

The organization-specific configurations are similar to the global configurations, but navigation paths to their task page is different. To access the task page for performing the organization-specific configurations:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 10-8.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

A list of organizations matching the search criteria (similar to Figure 10-9) appears.

5. Under the **Organization** column, click the `<ORGANIZATION_NAME>` link for the required organization.

The Organization Information page (similar to Figure 11-1) appears.

Figure 11-1 Organization Information Page

Arcot Administration Console

Welcome [RLAURIE](#) (DEFAULTORG) | [Logout](#)
Last Login Time

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations
● Search Organization

Basic Organization Information
○ [Organization Details](#)
○ [Basic Authentication Policy](#)

Organization Name: DEFAULTORG Display Name: DEFAULT ORGANIZATION Status: Active

Basic Organization Information | RiskFort Configuration

Organization Information
Edit the required fields and click Next to save the changes.

Organization Details

Organization Name: DEFAULTORG

Display Name:

Description:

Administrator Authentication Mechanism: Basic User Password

Date Created: 07/02/2010 05:02:51 GMT

Last Modified: 07/02/2010 05:10:12 GMT

Default Organization: Yes

6. Activate the **RiskFort Configuration** tab.

The organization-specific configuration links are displayed in the tasks pane (Figure 11-2).

Figure 11-2 Organization-Specific RiskFort Configurations

The screenshot displays the Arcot Administration Console interface. The top navigation bar includes 'Users and Administrators', 'Organizations', 'Reports', and 'Case Management'. The 'Organizations' tab is active, showing 'Manage Organizations' with a sidebar menu containing 'Manage Organizations', 'RiskFort Configuration', 'Ruleset', 'Rules', 'Data Upload', 'Scoring', and 'Migrate to Production'. The main content area shows the 'Create Ruleset' page for the 'DEFAULTORG' organization. It includes fields for 'Organization Name', 'Display Name', and 'Status'. Below this, there are tabs for 'Basic Organization Information' and 'RiskFort Configuration'. The 'Create Ruleset' section has a text input for 'Name' and an 'Advanced Options' section with a checkbox for 'Copy from an Existing Ruleset' and a dropdown menu. A 'Create' button is at the bottom right.

7. Configure and assign the required rulesets and risk evaluation rules.



Note: See [Chapter 7, “Managing Global Rule Configurations”](#) for detailed information on how to configure the required rules and assign them, as needed. The operations discussed in [Chapter 7, “Managing Global Rule Configurations”](#) are for global level, however the configurations discussed in this chapter are for organization level, the configurations for both are same only the approach to access the task page is different as explained at the beginning of this section.

Creating Rulesets

As discussed in section, “[Understanding Rulesets](#)” on page 7-78, a ruleset is a collection of rules configured by a Global Administrator (GA) or an Organization Administrator (OA.)



Important: If created by a GA, a ruleset is *only available for copying for individual organizations*. Therefore, an OA must either create a new ruleset by copying the global ruleset, or must re-create the ruleset again at the organization-level.

See “[Creating Rulesets](#)” on page 7-79 for detailed information on how to create a ruleset.



Important: After you create a ruleset, you *must* migrate it to production for it to be available for activation.

Assigning Rulesets

After an OA creates a ruleset for their organization and migrates it to production, you must activate this ruleset for an organization within your scope for it to take effect. To assign an existing ruleset to the current organization:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page ([Figure 11-3.](#))

Figure 11-3 Search Organization Page

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations
● **Search Organization**

Search Organization

Enter the (full or partial) Display Name of the organization that you want to search.

Organization:

Initial: ☐ Active: ☒ Inactive: ☐ Deleted: ☐ [Search](#)

- Enter the complete or partial information of the organization you want to search and click the **Search** button.

A list of organizations matching the search criteria (similar to [Figure 11-4](#)) appears.

Figure 11-4 Search Organization Page: Result

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | **Organizations** | Reports | Case Management

Manage Organizations

Manage Organizations
● **Search Organization**

Search Organization

Click the Organization Name link to view or edit the details of the selected organization. To enable, disable, or delete multiple organizations, select the required organizations and click the applicable button.
Tip: You can also reorder the list of organizations by clicking the Organization column heading.

Organization:

Initial: ☐ Active: ☒ Inactive: ☐ Deleted: ☐ [Search](#)

Select Organizations to Modify

	Organization	Display Name	Description	Status
☐	HSBC	HSBC		Active
☐	DEFAULTORG	DEFAULT ORGANIZATION	This is the initial default Organization.	Active
☐	SAFEBANK	Safe Bank		Active

[Activate](#) [Deactivate](#) [Delete](#)

- Under the **Organization** column, click the `<ORGANIZATION_NAME>` link for the required organization.

The Organization Information page (similar to [Figure 11-1](#)) appears.

6. Activate the **RiskFort Configuration** tab.
7. Under the **Ruleset** section, click the **Assign Ruleset** link.

The Assign Ruleset page ([Figure 11-5](#)) appears.

Figure 11-5 Assign Ruleset Page

The screenshot shows the Arcot Administration Console interface. The top navigation bar includes 'Users and Administrators', 'Organizations' (selected), 'Reports', and 'Case Management'. The left sidebar lists various configuration options under 'Manage Organizations', 'RiskFort Configuration', 'Ruleset', 'Rules', 'Data Upload', 'Scoring', and 'Migrate to Production'. The main content area displays the 'Assign Ruleset' page for the organization 'DEFAULTORG'. It shows the current assigned ruleset as 'DEFAULTORG - DEFAULT' and a dropdown menu to select a new ruleset. A 'Save' button is present at the bottom of the selection area.

8. Select the ruleset that you want to activate from the **Select Ruleset to Assign** list.
9. Click **Save** to make the specified ruleset active for the current organization.

Using Global Configurations

Although you can change the rule configurations individually for every organization in your scope, chances are that most of your organizations might be using the same configuration settings over and over again. Also, setting rule configurations for individual organizations can be a cumbersome

task if there are large number of organizations configured. In this case, you might want to tweak the global configurations set by a GA for the rules so that you do not need to specify the same setting every time.

When a GA, who has scope to your organizations, sets rule configurations at the global level, then all your organizations inherit these settings. You can use these settings either *by referring to them* or *by creating a copy*.

Use the **Advanced Options** section that you see on the configuration page of each rule. When you display a rule configuration page, you will see the + **Advanced Configuration** section on the page. The section is collapsed, and you will need to click on the + sign to expand the section and see the available options (Figure 11-6.)

Figure 11-6 The Advanced Options Section (Available On All Rule Configuration Pages)

As shown in Figure 11-6, you have the following two options available to use the global configurations set by your GA. You can only use one of them:

- **Use Own:** If you select this option, then you can specify your own configuration values.

RiskFort also enables you to modify your existing ruleset by copying the configuration or data from an existing ruleset. To use this option, select **Use Own**, select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the **Ruleset Name** list.



Note: The changes that you make on this page will *not* affect the ruleset that you are copying from.

- **Refer an Existing Ruleset:** If you select this option, then RiskFort enables you to use the ruleset that you specify as-is. Note that the you *cannot make any changes* if you select this option.

To use this option, select **Refer an Existing Ruleset** and then select the name of the ruleset whose configuration that you want to refer to from the **Ruleset Name** list.

Configuring RiskFort for An Organization

In addition to creating and assigning rulesets, as an Organization Administrator (OA), you can perform most of the tasks mentioned in [Chapter 7, “Managing Global Rule Configurations”](#). These include:

- Configuring the out-of-box rules for the organizations in your scope.
See [Chapter 7, “Managing Global Rule Configurations”](#) for detailed steps.
- Configuring scoring and migrating configurations to production for the organizations in your scope.
See [Chapter 8, “Configuring Scoring”](#) for detailed steps.
- Deploying Add-On rules for the organizations in your scope.
See [Chapter 12, “Working with Add-On Rules”](#) for detailed steps.
- Configuring Callouts for the organizations in your scope.
See [Chapter 9, “Configuring Callouts”](#) for detailed steps.

Chapter 12

Working with Add-On Rules



Important: All the configurations and tasks discussed in this chapter should primarily be performed by **Organization Administrators**. See section, “[Accessing Organization-Specific RiskFort Configurations](#)” in [Chapter 11](#) for more information to access the task page for performing the organization-specific configurations.

If required, these steps can also be performed by **Global Administrators**, however they must be performed at the *organization-level* (through the **Organizations** tab.)

The out-of-box [Evaluation Rules](#) in RiskFort are generic and are configured to evaluate risk for typical transactions. If your application needs to evaluate risk based on these generic rules, then you may get a lot of false positives or false negatives. You can also tweak the scores and priority of the default rules or create Whitelists and Blacklists to improve the results, but this might not be sufficient in all cases. In such cases, you need custom or industry-specific rules that are significantly different than those that RiskFort provides out-of-the-box. These terminating rules are referred to as *Add-On rules*.



Important: Add-On rules are run only *after* the out-of-the-box risk evaluation rules have finished executing. However, their scoring priority can be higher than that of out-of-the-box rules.

This chapter walks you through the basics of Add-On rules and then guides you through the process of configuring them to meet your business-specific requirements:

- [Understanding Add-On Rules](#)
- [Data Elements and Operators Used for Building Add-On Rules](#)
- [Add-On Rule Examples](#)
- [Working with Add-On Rules](#)
- [Uploading Add-On Rule List Data](#)



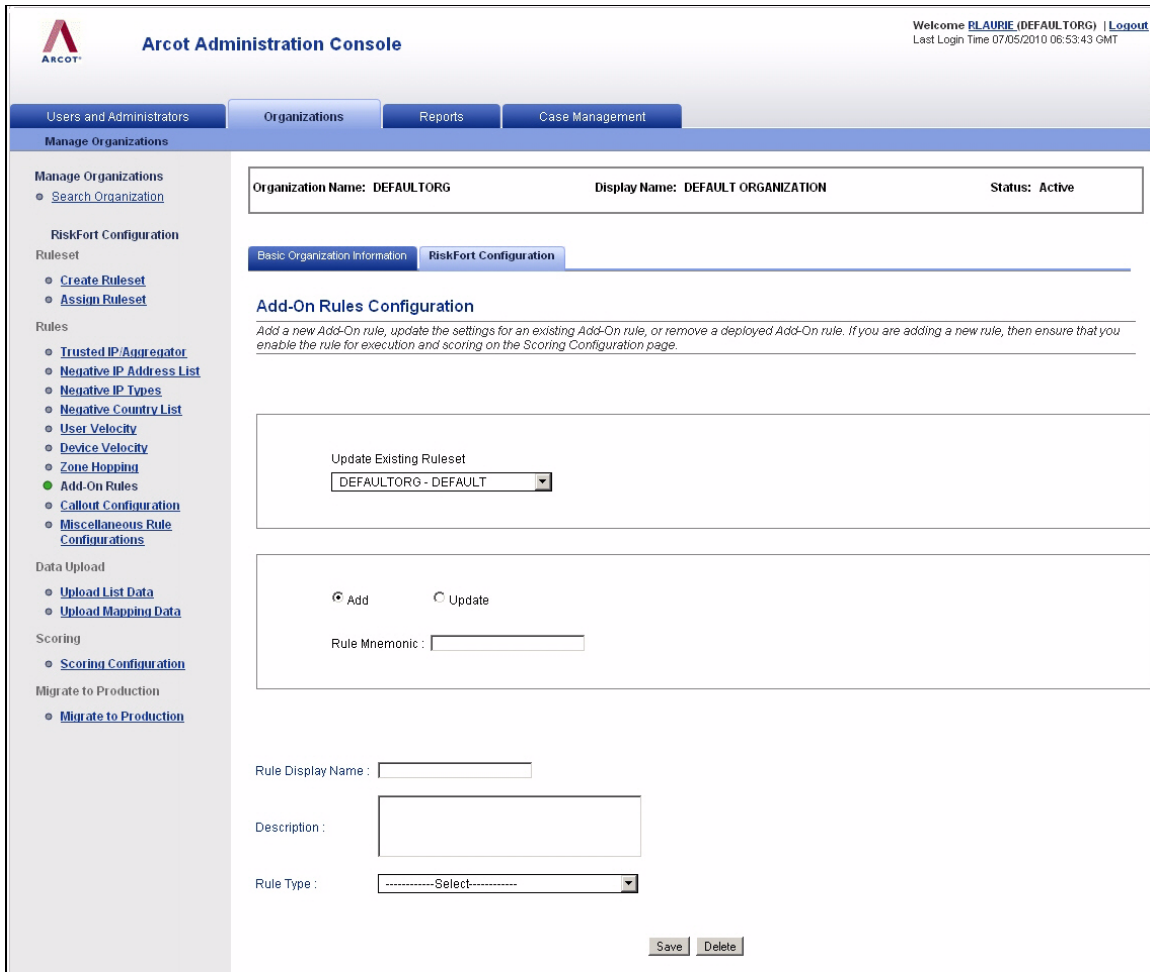
Note: The administrator performing configuration-related activities *must* have privileges to perform these operations. For more information on the privileges available to administrators at each level, refer to the section, “[Summary of Administrative Privileges](#)” in [Chapter 1](#).

After you update any of the **default** (out-of-box) configurations for RiskFort, the changes are not immediately **active** (available to your end users.) You *must* use the **Migrate to Production** link in the side-bar menu to “move” all **proposed** configuration changes to your production database. See the “[Migrating to Production](#)” section to understand the concept of *default*, *proposed*, and *active* configuration data used by RiskFort.

Understanding Add-On Rules

Unlike the pre-defined out-of-box rules, Add-On rules are *not* deployed automatically when you install RiskFort. The Master Administrator (MA) must first add a corresponding **Rule Type** (as discussed in [Chapter 6](#), “[Preparing for Add-On Rules: Working with Rule Types](#)”) for your Add-On rule, then (as a Global or Organization Administrator) you must specify the rule-specific settings by using the Add-On Rules Configuration page ([Figure 12-1](#)).

Figure 12-1 Add-On Rules Configuration Page



Arcot Administration Console

Welcome **PLAURIE (DEFAULTORG)** | [Logout](#)
Last Login Time 07/05/2010 06:53:43 GMT

Users and Administrators | **Organizations** | **Reports** | **Case Management**

Manage Organizations

Manage Organizations

- [Search Organization](#)

RiskFort Configuration

Ruleset

- [Create Ruleset](#)
- [Assign Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address List](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- Add-On Rules**
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Organization Name: DEFAULTORG Display Name: DEFAULT ORGANIZATION Status: Active

Basic Organization Information | **RiskFort Configuration**

Add-On Rules Configuration

Add a new Add-On rule, update the settings for an existing Add-On rule, or remove a deployed Add-On rule. If you are adding a new rule, then ensure that you enable the rule for execution and scoring on the Scoring Configuration page.

Update Existing Ruleset

DEFAULTORG - DEFAULT

☒ Add ☐ Update

Rule Mnemonic :

Rule Display Name :

Description :

Rule Type :

This page (Figure 12-1) also enables you to combine the out-of-box rules (such as Velocity rules) or your uploaded lists with transaction and system elements, mathematical operators, and boolean functions to identify fraudulent transactions.



Note: After an Add-On rule is deployed, you *must* enable it by using the Scoring Configuration page (Figure 8-1 in Chapter 8, “Configuring Scoring”) for it to take effect.

Data Elements and Operators Used for Building Add-On Rules

You need the following elements to build an Add-On rule:

- [Data Elements](#)
- [Logical Operators](#)
- [Additional Input Elements Used by Add-On Rules](#)

Data Elements

To deploy an Add-On rule, you require:

- **Rule Mnemonic:** A short name for the rule that is used for logging purposes and in APIs. The maximum length of the mnemonic is 15 characters and no spaces are allowed.
- **Rule Display Name:** The display name that will appear in the Scoring Configuration screen.
- **Rule Type:** The type of the rule, which can either be pre-existing or can be defined by the MA.



Note: See [“System-Defined Rule Types” in Chapter 6](#) for more information on the rule types that are shipped out-of-the-box.

Depending on the Rule Type you select, the following additional data elements are available to you. These include:

- **Currency AND Amount:** Used by the AMOUNT_CHECK rule type.
- **Duration:** Used by CARDHOLDER_MERCHANT_AMOUNT, IPADDRESS_MERCHANT_AMOUNT, IP_VELOCITY, and TRANSACTION_TYPE_CHECK rule types.
- **Frequency:** Used by CARDHOLDER_MERCHANT_AMOUNT, IPADDRESS_MERCHANT_AMOUNT, and IP_VELOCITY rule types.
- **Rules:** All built-in and Add-On rules defined so far. Used by COMBINATION_RULE type.
- **Tag Name:** Parameter definition. Used by DERIVED_LIST_LOOKUP, NUMERIC_COMPARISON, SIMPLE_LIST_LOOKUP

- **Enable List Caching:** **0** if not, and **1** if yes. Used by DERIVED_LIST_LOOKUP and SIMPLE_LIST_LOOKUP rule types.
- **Enable Mapping Caching:** **0** if not, and **1** if yes. Used by DERIVED_LIST_LOOKUP rule type.
- **Mapping Data Set:** Dataset (or mapping list) used by the Add-On rule. Used by DERIVED_LIST_LOOKUP, MERCHANT_CATEGORY_LOOKUP, and MERCHANT_REGION_LOOKUP rule types.
- **Disable Processing, Upper Limit for ALLOW, and Upper Limit for INCREASE AUTH:** Used by GDP (or RiskFort Model) rule type.
- **Threshold:** Used by NUMERIC_COMPARISON rule type.
- **Previous Transaction Types:** All transactions supported by Arcot TransFort. Used by the TRANSACTION_TYPE_CHECK rule type.

Logical Operators

Based on the Rule Type, the following categories of logical operators are currently supported:

- **Expression:** Include **AND**, **OR**, **NOT**, **(**, and **)** operators. Used by the COMBINATION_RULE type.
- **Match Type:** Possible operators include **EXACT** and **PARTIAL**. Used by the DERIVED_LIST_LOOKUP and SIMPLE_LIST_LOOKUP rule types.
- **LookUp Type:** Possible operators include **IN_LIST** and **NOT_IN_LIST**. Used by the DERIVED_LIST_LOOKUP and SIMPLE_LIST_LOOKUP rule types.
- **Operator:** Possible operators include **EQ** (=), **NEQ** (!=), **GTE** (>=), **LTE** (<=), **GT** (>), and **LT** (<). Used by the NUMERIC_COMPARISON rule type.

Additional Input Elements Used by Add-On Rules

Add-On rules typically use *Additional Inputs*. These Additional Inputs are additional name-value custom parameters that capture the real-time input from each transaction, and are then processed by the Add-On rule for successful risk evaluation.

Important Notes Related to Additional Inputs

- RiskFort uses IP address, DeviceID, MFP, **username**, and **transactiontype** as base elements. Any element other than these out-of-the-box elements is considered an Additional Input.

- Additional Inputs are programmatic elements, and *cannot* be configured by using the Administration Console.
- An Add-On rule may not use any Additional Inputs at all.

Add-On Rule Examples

The following subsections illustrate how you can combine out-of-box RiskFort rules or your Add-On rules to define custom combination rules by using multiple factors and conditions.



Note: The rule (for example, [SAFE_COUNTRIES](#)) that you see in the following examples represent uploaded lists (*_LIST_LOOKUP).

High Amount Check

Consider the following details for an AMOUNT_CHECK rule that must check for transaction amounts more than \$500:

- **Rule Mnemonic:** HIGHAMTCHK
- **Rule Display Name:** High Amount Check
- **Description:** This rule checks for high transaction amounts that exceed \$500.
- **Rule Type:** AMOUNT_CHECK
- **Amount:** 500

This example rule performs the following:

1. Parses the [AdditionalInput](#) string (say [Amount=750](#)) that is passed in the [evaluateRisk\(\)](#) API call by the tag called [Amount](#) and extract the value of this tag in a variable, say [ActualAmount](#).



Note: Refer to the Javadocs for details on parsing the [AdditionalInput](#) elements.

2. Extracts the parameter value ([500](#)) for the rule, and store it in a variable, say [ParameterAmount](#).

- Returns **Matched** because **ActualAmount** (750) , in this case, is greater than **ParameterAmount** (500).

High User Velocity from Unexpected Locations

Consider that the **SAFE_COUNTRIES** refers to a **SIMPLE_LIST_RULE** (where some of the elements are US,CA, UK, DE), then you can define a custom **COMBINATION_RULE** to determine transactions with high User Velocity from unusual locations as:

```
USERVELOCITY AND NOT SAFE_COUNTRIES
```

High Device Velocity from Unexpected Locations

Similar to the preceding example, you can define a custom **COMBINATION_RULE** to determine transactions with high Device Velocity from unusual locations as:

```
DEVICEVELOCITY AND NOT SAFE_COUNTRIES
```

Wire Transfers from Unexpected Locations

Consider that you have created an Add-On rule called **HIGHAMTCHK** (discussed in “[High Amount Check](#)” earlier.) Also, if the **SAFE_COUNTRIES** rule uses a list of countries considered to be origin of safe transfers, then you can define a custom **COMBINATION_RULE** to track low-value or high-amount wire transfers from unusual locations as:

```
(HIGHAMTCHK OR Amount < 20) AND NOT SAFE_COUNTRIES
```

Working with Add-On Rules



Important: Before you deploy, edit, or remove an Add-On rule, you must ensure that the Master Administrator (MA) has added the corresponding Rule Type (as discussed in “[Working with Custom Rule Types](#)” on page 6-66). Only then you can proceed with specifying rule-specific settings by using the **Add-On Rules Configuration** page ([Figure 12-1](#)).

Use the Add-On Rules Configuration page for:

- [Deploying an Add-On Rule](#)
- [Editing the Attributes of a Deployed Add-On Rule](#)
- [Deleting a Deployed Add-On Rule](#)

Deploying an Add-On Rule

To deploy an Add-On rule:

1. Ensure that you are logged in as an OA or a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the Add-On rule.
5. Click the **RiskFort Configuration** tab.
6. Under the **Rules** section on the side-bar menu, click the **Add-On Rules** link.

The Add-On Rules Configuration page appears, as shown in [Figure 12-1](#).

7. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.

The configuration information for the specified ruleset appears.

8. Select the **Add** option to add a new Add-On rule.
9. Specify a short name for the rule in the **Rule Mnemonic** field.



Note: The maximum length of the Mnemonic is 15 characters and no spaces are allowed.

10. Specify the name for the new rule in the **Rule Display Name** field.
This name will be used in the Scoring Configuration screen and the corresponding Add-On Rule Report.
11. Enter useful information related to the Add-On rule for later reference in the **Description** field.

12. From the **Rule Type** list, select one of the pre-existing rule types or a custom rule type defined by the Master Administrator.



Note: See [“Working with Custom Rule Types”](#) on page 6-66 for more information.

Based on the selected Rule Type that the MA created, additional fields might appear.

13. Specify the required information in the new fields that might appear.
14. Click **Save** to deploy the rule.
15. Enable the Add-On rule you just deployed. Refer to [“Configuring Scoring”](#) for instructions to do so.

The Add-On rule you just deployed is yet not active, and not available to your end users.

16. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production”](#) for instructions to do so.

Editing the Attributes of a Deployed Add-On Rule

To edit the attributes of a deployed Add-On rule, perform the following steps:

1. Ensure that you are logged in as an OA or a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization’s name to which you want to apply the Add-On rule.
5. Click the **RiskFort Configuration** tab.
6. Under the **Rules** section on the side-bar menu, click the **Add-On Rules** link.

The Add-On Rules Configuration page appears, as shown in [Figure 12-1](#).

7. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.

The configuration information for the specified ruleset appears.

8. Select the **Update** option to edit the settings for a deployed Add-On rule.
9. Select the rule that you want to update from the **Add-On Rule** list.

The additional fields defined for the rule appear.

10. Make the required changes.
11. Click **Save** to update the rule.
12. Enable the Add-On rule you just deployed. Refer to [“Configuring Scoring”](#) for instructions to do so.

The Add-On rule you just deployed is yet not active, and not available to your end users.

13. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production”](#) for instructions to do so.

Deleting a Deployed Add-On Rule

To delete a deployed Add-On rule, perform the following steps:

1. Ensure that you are logged in as an OA or a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization’s name to which you want to apply the Add-On rule.
5. Click the **RiskFort Configuration** tab.
6. Under the **Rules** section on the side-bar menu, click the **Add-On Rules** link.

The Add-On Rules Configuration page appears, as shown in [Figure 12-1](#).

7. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.

The configuration information for the specified ruleset appears.

8. Select the **Update** option to display the deployed Add-On rules.
9. Select the rule that you want to delete from the **Add-On Rule** list.
10. Click **Delete** to remove the rule.

The changes are yet not active, and not available to your end users.

11. Enable the Add-On rule you just deployed. Refer to [“Configuring Scoring”](#) for instructions to do so.

The Add-On rule you just deployed is yet not active, and not available to your end users.

12. To make the changes active, you must migrate them to production.

Refer to [“Migrating to Production”](#) for instructions to do so.

Uploading Add-On Rule List Data



Important: If you are performing any of the tasks mentioned in this section, then you must ensure that you have first deployed a corresponding Add-On rule for the list. See [“Deploying an Add-On Rule”](#) for detailed instructions to do so.

If an Add-On rule that you deployed ([“Deploying an Add-On Rule” on page 12-186](#)) requires additional data in form of simple or derived list, then you must perform the tasks in this section. Depending on your list type, this might include:

- [Uploading \(Simple\) List Data](#)
- [Uploading Mapping \(Derived List\) Data](#)

Uploading (Simple) List Data

To upload the data for an Add-On rule that uses SIMPLE_LIST_LOOKUP Rule Type:

1. Ensure that you are logged in as an OA or a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under the **Select Organizations to Modify** section, click the link with the organization’s name to which you want to apply the Add-On rule.
5. Click the **RiskFort Configuration** tab.
6. Under the **Data Upload** section on the side-bar menu, click the **Upload List Data** link.
The Upload Rules List Data page appears.
7. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. From the **Select Dataset** list, select the **<Rule Mnemonic>** that you specified while creating the corresponding Add-On rule.
The updated Upload Rules List Data page ([Figure 12-2](#)) is displayed.

9. In the **Upload File Or Enter Data** section, Select the appropriate mode for writing data:

- **Append:** This option appends the data that you are uploading to an list or dataset.



Note: You must select this option if the list does not exist.

- **Replace:** This option overwrites the existing data in the specified list or dataset.

10. Perform *one* of the following:

- Click **Browse** to navigate to the data file that contains the list of entries (separated by a newline character.)

or

- Type in the entries in the **Enter Data** field, if a data file does not exist.



Important: Ensure that the entries are separated by a newline character (ENTER).

11. Click **Upload** to complete the task.

Figure 12-2 Upload Rules List Data Page


Arcot Administration Console

Welcome [RLAUIPIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/05/2010 09:28:14 GMT

[Users and Administrators](#)
[Organizations](#)
[Reports](#)
[Case Management](#)

Manage Organizations

Manage Organizations

- [Search Organization](#)

RiskFort Configuration

- [Create Ruleset](#)
- [Assign Ruleset](#)

Rules

- [Trusted IP/Aggregator](#)
- [Negative IP Address List](#)
- [Negative IP Types](#)
- [Negative Country List](#)
- [User Velocity](#)
- [Device Velocity](#)
- [Zone Hopping](#)
- [Add-On Rules](#)
- [Callout Configuration](#)
- [Miscellaneous Rule Configurations](#)

Data Upload

- [Upload List Data](#)
- [Upload Mapping Data](#)

Scoring

- [Scoring Configuration](#)

Migrate to Production

- [Migrate to Production](#)

Organization Name: DEFAULTORG Display Name: DEFAULT ORGANIZATION Status: Active

[Basic Organization Information](#)
[RiskFort Configuration](#)

Upload Rules List Data

Select the dataset and upload a file or enter data.

Update Existing Ruleset

Select Dataset:

Upload File Or Enter Data

☒ Append ☐ Replace

Upload Data File: [Browse...](#)

--OR--

Enter Data:

[Upload](#)

Uploading Mapping (Derived List) Data

To upload the data for an Add-On rule that uses DERIVED_LIST_LOOKUP, MERCHANT_CATEGORY_LOOKUP, or MERCHANT_REGION_LOOKUP Rule Type:

1. Ensure that you are logged in as an OA or a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under the **Select Organizations to Modify** section, click the link with the organization's name to which you want to apply the Add-On rule.
5. Click the **RiskFort Configuration** tab.
6. Under the **Data Upload** section on the side-bar menu, click the **Upload Mapping Data** link.
The Upload Rules Mapping Data page appears.
7. From the **Update Existing Ruleset** list, select the ruleset for which this configuration is applicable.
The configuration information for the specified ruleset appears.
8. From the **Select Dataset** list, select the *<Mapping Data Set>* that you specified while creating the corresponding Add-On rule.
The updated Upload Rules List Data page ([Figure 12-2](#)) is displayed.

Figure 12-3 Upload Rules Mapping Data Page


Arcot Administration Console
Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/05/2010 09:28:14 GMT

[Users and Administrators](#)
[Organizations](#)
[Reports](#)
[Case Management](#)

Manage Organizations

Manage Organizations

- [Search Organization](#)

RiskFort Configuration

- Ruleset**
 - [Create Ruleset](#)
 - [Assign Ruleset](#)
- Rules**
 - [Trusted IP/Aggregator](#)
 - [Negative IP Address List](#)
 - [Negative IP Types](#)
 - [Negative Country List](#)
 - [User Velocity](#)
 - [Device Velocity](#)
 - [Zone Hopping](#)
 - [Add-On Rules](#)
 - [Callout Configuration](#)
 - [Miscellaneous Rule Configurations](#)
- Data Upload**
 - [Upload List Data](#)
 - [Upload Mapping Data](#)
- Scoring**
 - [Scoring Configuration](#)
- Migrate to Production**
 - [Migrate to Production](#)

Organization Name: DEFAULTORG **Display Name:** DEFAULT ORGANIZATION **Status:** Active

[Basic Organization Information](#)
[RiskFort Configuration](#)

Upload Rules Mapping Data

Select the dataset and upload a file or enter data.

Update Existing Ruleset
 DEFAULTORG - DEFAULT

Select Dataset: MERCHANT_CATEGORY_MAPPING

Upload File Or Enter Classification Data

☒ Append
 ☐ Replace

Upload Data File: [Browse...](#)

--OR--

Enter Data:

[Upload](#)

9. In the **Upload File Or Enter Classification Data** section, select the appropriate mode for writing data:

- **Append:** This option appends the data that you are uploading to an list or dataset.



Note: You must select this option if the list does not exist.

- **Replace:** This option overwrites the existing data in the specified list or dataset.

10. Perform *one* of the following:

- Click **Browse** to navigate to the data file that contains the list of entries (separated by a newline character.)

or

- Type in the entries in the **Enter Data** field, if a data file does not exist.



Important: Ensure that the entries are separated by a newline character (ENTER).

11. Click **Upload** to complete the task.

Chapter 13

Managing Administrators

The types of administrators and their roles and responsibilities depend on the size of your deployment. A small, single-organization deployment can have just one Master Administrator (MA) and a Global Administrator (GA) who administers the organization for end users. On the other hand, a very large multi-organization deployment can find it necessary to have multiple GAs who, based on the complexity of the deployment and the number of end users, can further delegate their organization and user management duties among several Organization Administrators (OAs) and User Administrators (UAs).

See “Supported Roles” on page 1-4 for information on supported administrative roles. Table 1-2 on page 1-11 provides a quick summary of tasks each of these administrators can perform. This chapter covers the following administrator management operations:

- [Creating Administrators](#)
- [Changing Profile Information for Administrator Accounts](#)
- [Searching Administrators](#)
- [Updating Administrator Account Information](#)
- [Disabling Administrator Accounts](#)
- [Enabling Administrator Accounts](#)
- [Deleting Administrator Accounts](#)



Note: In addition to all the operations discussed in this chapter, the Master Administrator has a privilege to create “[Custom Roles](#)” on page 1-14 that are derived from the existing default roles supported by WebFort.

Creating Administrators

Privileges Required to Create Administrators

An administrator can create other administrators who belong to the same level or to the lower levels in the administrative hierarchy *and* have the same or lesser scope. For example:

- Master Administrator can create all other types of administrators.
- Global Administrators (GAs) can create the following *within* their scope:
 - Other GAs
 - Organization Administrators (OAs)
 - User Administrators (UAs)
- OAs can create the following *within* their scope:
 - Other OAs
 - UAs
- UAs can create other UAs *within* their scope.

To create an administrator account with Basic Username-Password credential:

1. Ensure that you are logged in with the required privileges and scope to create the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Create Administrator** link to display the Create Administrator page ([Figure 13-1.](#))

Figure 13-1 Create Administrator: Page 1

Arcot Administration Console

Welcome **PLAURIE** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- **Create Administrator**
- [Search Users and Administrators](#)

Create Administrator

Enter the details for the administrator that you want to create.

Administrator Details

User Name: *

Organization: *

First Name: *

Middle Name:

Last Name: *

Email Address: *

Phone Number:

4. In the **Administrator Details** section, enter the details of the administrator. [Table 13-1](#) explains the fields on this page.

Table 13-1. Inputs for Creating Administrators

Input	Description
User Name	The unique user name for the administrator.
Organization	The display name of the organization to which the administrator will belong. Note: This is <i>not</i> the organization that this administrator will manage.
First Name	The first name of the administrator.
Middle Name (optional)	The middle name, if any, of the administrator.
Last Name	The last name of the administrator.

Table 13-1. Inputs for Creating Administrators

Input	Description
Email Address	The email address of the administrator.
Phone Number (optional)	The phone number to contact the administrator.

5. Click **Next** to proceed.

The next page ([Figure 13-2](#)) to Create Administrator appears.

Figure 13-2 Create Administrator: Page 2

Arcot Administration Console

Welcome [RLAURIE \(DEFAULT ORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- Create Administrator
- [Search Users and Administrators](#)

User Name: DCHEN Organization: DEFAULT ORGANIZATION Status: Initial

Create Administrator

Set the Administrator's Role, Scope, and Password credential.
Note: To reset the credential, the target administrator will need to go through the reset flow.

Role

Role:

Set Password

Password:

Confirm Password:

Manages

All Organizations: ☐

Available Organizations

- DEFAULT ORGANIZATION
- HSBC
- Safe Bank

Selected Organizations

6. On this page:
 - Specify the role of the new administrator from the **Role** drop-down list.
 - In the **Manages** section, select the organizations that the administrator will have scope on:
 - Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.
 - or
 - Select the required organizations from the **Available Organizations** list and click the > button to add these organization to the **Selected Organizations** list.

The **Available Organizations** list displays *all* the organizations that are available in the scope of the administrator creating this new account. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.
7. Click **Create** to save the changes, create the account and activate it.
8. Communicate the new password to the administrator.

Changing Profile Information for Administrator Accounts

The profile information for an account includes:

- Personal information (first, middle, and last names and contact information)
- Password for the account
- Preferred organization (the organization that will be selected by default in the **Organization** fields for all administrator-related tasks that you might perform in future.)



Note: An administrator can change their account's profile information at any time. To change the information for any other administrative account, see [“Updating Administrator Account Information”](#).

To change the administrator profile information for your account, if it was created with basic Username-Password credential:

1. Ensure that you are logged in to your account.
2. In the **Header** frame, click the <ADMINISTRATORNAME> link to display the My Profile page ([Figure 13-3.](#))

3. This page contains the following three sections:

- Personal Information

This section enables you to change the first name, last name, middle name, email ID, and the phone number.

- Change Password

This section enables you to set a new password.

- Administrator Preferences

In this section you can set the default organization that the administrator will handle.

Figure 13-3 My Profile Page

Arcot Administration Console

Welcome **RLAURIE** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

User Name: RLAURIE Organization: DEFAULTORG Role: Organization Adminis...

My Profile
Update your personal details and preferences.

Personal Information

First Name: *
Middle Name:
Last Name: *
Email: *
Phone:

Change Password

Current Password:
New Password:
Confirm Password:

Administrator Preferences

Enable Preferred Organization: ☐
Preferred Organization:
Time Zone:

4. Edit the required settings in the sections on this page:
 - a. Edit the fields in the **Personal Information** section, as needed.
 - b. If you want to change the current password, then in the **Change Password** section enter the **Current Password** and specify new password in the **New Password** and **Confirm Password** fields.

- c. In the **Administrator Preferences** section:
 - Select the **Enable Preferred Organization** option, and select an organization from the **Preferred Organization** list. This organization will be selected for all administrator-related tasks that you perform from now on.
 - Select the required option from the **Time Zone** list. This timestamp will be reflected in the **Last Login** information in the console header and all reports and Case Management activities (if available) from now on.
5. Click **Save** to change the profile information.

Searching Administrators



Note: As long as you do not need to update, activate, or deactivate an administrative account, you do not need privileges to search. However, you *must* have the scope over the organizations that the administrator belongs to. For example, a UA can search for administrators in the target organization *if* that organization is in their purview.

To search for administrators with the specified criteria:

1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page ([Figure 13-4.](#))

Figure 13-4 Search Users and Administrators Page

The screenshot shows the Arcot Administration Console interface. At the top, there is a header with the Arcot logo, the title "Arcot Administration Console", and a user welcome message: "Welcome [RLAURIE \(DEFAULTORG\)](#) | [Logout](#)". Below the header, a navigation bar contains four tabs: "Users and Administrators" (selected), "Organizations", "Reports", and "Case Management". Under the "Users and Administrators" tab, there is a sub-section "Manage Users and Administrators" with two links: "Create Administrator" and "Search Users and Administrators" (which is highlighted with a green dot). The main content area is titled "Search Users and Administrators" and includes a tip: "Specify the search criteria to display the list of users. Use the Advanced Search link to additionally search on Status or Role. Tip: You need not enter the complete values in the fields. Also, you can specify the organization's Display Name to search for the user in an organization." Below the tip is a search form with five input fields: "First Name", "Last Name", "User Name", "Organization", and "Email". To the right of these fields are two buttons: "Search" and "Advanced Search".

4. Specify the search criteria to display the list of administrators. You can:
 - Search for administrators by specifying the partial or complete information of the administrator in the fields on this page.
 - Search for administrators by specifying the organization's Display Name.
 - Search for administrators by not specifying any criteria and just clicking **Search**.
 - Click the **Advanced Search** link to display the Advanced Search page (Figure 13-5) to search for the required administrators by specifying their Status or Role.

Figure 13-5 Advanced Search Page

Arcot Administration Console

Welcome **BLAURIE (DEFAULTORG)** | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Advanced Search

Click the User Search Criteria tab to specify the type of credential you want to base your search on.

User Search Criteria

User Details

First Name:

Middle Name:

Last Name:

User Name:

Organization:

Email Address:

User Status

Include Active Users: ☒

Include Inactive Users: ☐

Include Deleted Users: ☐

Available Roles

Role:

User
Customer Service Rep(CSR)
Fraud Analyst
Global Administrator

Search

5. Specify the required details of the administrators and click **Search**.

A list of administrators matching the search criteria appears.

Updating Administrator Account Information



Note: To be able to update an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can update any account. GAs can update all the accounts (including other GAs), *except* for the MA account, in their scope. The OAs can update all other OA accounts and the UA accounts in their purview, while UAs can only update the accounts of their peers within their scope.

To update an administrator's basic details (such as first, middle, and last names, contact information) and their administrative role, password, and management scope:

1. Ensure that you are logged in with the required privileges to update the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the corresponding page ([Figure 13-4.](#))
4. Enter the partial or complete information of the administrator whose account you want to update (as discussed in the preceding section) and click **Search**.

A list of administrators matching the search criteria appears.

5. Click the *<user name>* link of the administrator whose account you want to edit.

The Basic User Information page similar to [Figure 13-6](#) appears.

Figure 13-6 Basic Administrator Information Page

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the text "Arcot Administration Console" is in the center. On the right, a welcome message reads "Welcome [BLAURIE \(DEFAULTORG\)](#) | [Logout](#)" with "Last Login Time 07/12/2010 11:16:24 GMT" below it. A navigation bar contains four tabs: "Users and Administrators" (selected), "Organizations", "Reports", and "Case Management". Below this, a sub-header reads "Manage Users and Administrators". On the left sidebar, under "Manage Users and Administrators", there are links for "Create Administrator" and "Search Users and Administrators". Below these, under "Basic User Information", the "User Details" option is selected and highlighted with a green dot. The main content area shows a summary box with "User Name: FANTONY", "Organization: DEFAULT ORGANIZATION", and "Status: Active". Below this is a tab labeled "Basic User Information". Underneath the tab is a box titled "User Information" containing the following details: First Name: Francis, Middle Name: N/A, Last Name: Antony, Email Address: fantony@arcot.com, Creation Date: 07/09/2010 09:12:09 GMT, Last Modified: 07/09/2010 09:12:09 GMT, and Phone Number: N/A. At the bottom of this box are two buttons: "Edit" and "Return to Search".

Arcot Administration Console

Welcome [BLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- **User Details**

User Name: FANTONY Organization: DEFAULT ORGANIZATION Status: Active

Basic User Information

User Information

First Name: Francis
Middle Name: N/A
Last Name: Antony
Email Address: fantony@arcot.com
Creation Date: 07/09/2010 09:12:09 GMT
Last Modified: 07/09/2010 09:12:09 GMT
Phone Number: N/A

[Edit](#) [Return to Search](#)

6. Click **Edit** to change the administrator information on this page, as shown in the following figure ([Figure 13-7](#).)

Figure 13-7 User Information Page

The screenshot shows the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title "Arcot Administration Console" is in the center. On the right, a welcome message says "Welcome [PLAURIE](#) (DEFAULTORG) | [Logout](#)" with the last login time "07/12/2010 11:16:24 GMT". Below the header is a navigation bar with tabs: "Users and Administrators" (selected), "Organizations", "Reports", and "Case Management". Under "Users and Administrators", there is a sub-tab "Manage Users and Administrators". On the left sidebar, under "Manage Users and Administrators", there are links: "Create Administrator", "Search Users and Administrators", "Basic User Information", and "User Details" (which is selected with a green dot). The main content area shows user information for "FANTONY". At the top, it displays "User Name: FANTONY", "Organization: DEFAULT ORGANIZATION", and "Status: Active". Below this is a section titled "Basic User Information" with a sub-section "User Information". A note states: "Edit the required user information. Click the Next button to reset their password and the scope of management, if this user belongs to an administrative role." The "Administrator Details" section contains the following fields: "Date Created: 07/09/2010 09:12:09 GMT", "Last Modified: 07/09/2010 09:12:09 GMT", "First Name: Francis", "Middle Name: ", "Last Name: Antony", "Email Address: fantony@arcot.com", and "Phone Number: ". At the bottom of this section are three buttons: "Save", "Next", and "Return to Search".

7. In the **Administrator Details** section, edit the required fields (**First Name, Middle Name, Last Name, Email Address, and Phone Number.**)
8. You can either click **Save** to save the changes made and return to the User Information page, *or* you can click **Next** to proceed with additional configurations.

If you click **Next**, then the Update Administrator page (Figure 13-8) appears.

Figure 13-8 Update Administrator Page

Arcot Administration Console

Welcome **PLAURIE** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- User Details**

User Name: FANTONY **Organization:** DEFAULT ORGANIZATION **Status:** Active

Basic User Information

Update Administrator

Update the details of the specified administrative user.
Note: To reset the credential, the target administrator will need to go through the reset flow.

Role

Role: *

Set Password

Password: *

Confirm Password: *

Manages

Manages

9. Edit the required fields on this page:

- Change the role of the administrator using the **Role** drop-down list.

- **Set Password** for the administrator.
- Select the organizations that administrator will manage. You can also remove the organization from the scope by moving the specific organization from **Selected Organizations** to **Available Organizations**.

10. Click **Save** to save the updates.

Disabling Administrator Accounts

To prevent an administrator from logging in to their account for security reasons, you can disable their account instead of deleting it. If you disable an administrator account, the administrator is locked out of their account, and cannot log in unless the account is re-enabled again.



Note: To be able to disable an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can disable any account, while GAs can disable all accounts (including other GAs), *except* the MA account, in their scope. The OAs can disable all other OA accounts and the UA accounts in their purview, while UAs can only disable the accounts of their peers within their scope.

To disable an administrator account:

1. Ensure that you are logged in with the required privileges to disable the administrative user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page ([Figure 13-4.](#))
4. Enter the partial or complete information of the administrator whose account you want to disable and click **Search**.

You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (GA, OA, or UA).

The Search Results page ([Figure 13-9](#)) appears, with all the matches for the specified criteria.

Figure 13-9 Search Results

Arcot Administration Console

Welcome [PLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- Search Users and Administrators**

Search Results

Click the [User Name](#) link to view or edit the details. To enable, disable, or delete multiple user accounts, select the users and click the applicable button.
Note: You can also reorder the user list by clicking the [User Name](#) column heading.

First Name Last Name User Name Organization Email

[Advanced Search](#)

Select Users to Modify ◀◀ 1 2 ▶▶

☐	User Name	Full Name	Organization	Email	Role	User Status
☐	FRANK	FNAME LNAME	DEFAULT ORGANIZATION	user@arcot.com	User	Active
☒	LWARD	Lauren Ward	DEFAULT ORGANIZATION	lward@arcot.com	Organization Adminis...	Active

Results 11-12 of 12

5. Select one or more administrators whose accounts you want to disable.
6. Click **Disable** to disable the selected administrator account.

Enabling Administrator Accounts

You might need to enable a disabled account. For example, you might disable an administrator account in case the administrator is on long vacation. This helps to prevent unauthorized access to that administrator's account.

You cannot search directly for disabled accounts by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You *must* perform an **Advanced Search** for such users and use the **Include Inactive Users** option to search.



Note: To be able to enable an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can enable any account, while GAs can enable all accounts (including other GAs), *except* the MA account, in their scope. The OAs can enable all other OA accounts and the UA accounts in their purview, while UAs can only enable the accounts for their peers within their scope.

To enable a disabled administrator account:

1. Ensure that you are logged in with the required privileges to enable the administrative user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 13-4.)
4. Click the **Advanced Search** link to search for users based on their status (active or inactive).
The Advanced Search page (Figure 13-5) appears.
5. Enter the partial or complete information of the administrator in **User Account** section.
6. In the **User Status** section, select the **Include Inactive Users** option to search for all inactive administrator accounts.
7. Click **Search** to display the list of all administrators matching the search criteria.
8. Select the administrators whose account you want to enable.
9. Click **Enable** to enable the administrator accounts.

Deleting Administrator Accounts

After an administrator account is deleted, all privileges associated with the administrator account are permanently deleted. As a result, the administrator can no longer log in to Administration Console. However, their account information and credentials *are not* removed from the system.

You cannot create a new administrator account with the same name as a previously deleted administrator account in the same organization, however you can create in different organization.



Note: To be able to delete an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can delete any account, while GAs can delete all accounts (including other GAs), *except* the MA account, in their scope. The OAs can delete all other OA accounts and the UA accounts in their purview.

However, UAs *cannot* delete their peers within their scope.

To delete an administrator account:

1. Ensure that you are logged in with the required privileges to delete the administrative user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 13-4.)
4. Enter the partial or complete information of the administrator whose account you want to delete and click **Search**.

You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (GA, OA, or UA).

The Search Results page (similar to Figure 13-9) appears, with all the matches for the specified criteria.

5. Select one or more administrators whose accounts you want to delete.
6. Click **Delete**.



Note: Even though you have deleted the administrator, their account information is still maintained in the database.

Chapter 14

Managing Users

RiskFort works with your application to manage strong authentication for administrators and end users. However, RiskFort *does not* allow you to create the end users directly through the Administration Console. For the purpose of migrating existing users and creating new users in RiskFort database as bulk operations, RiskFort provides extensive SDKs and Web Services. This process of creating users in RiskFort is known as *migration*.



Book: See section, "Enrollment Workflows" in Chapter 2 of the *Arcot RiskFort 2.2.6 Developer's Guide* to understand the workflows for user enrollment

Managing user information is a critical part of maintaining a secure system. The end user management operations supported by RiskFort for this purpose include:

- [Searching Users](#)
- [Updating User Information](#)
- [Promoting Users to Administrators](#)
- [Disabling User Accounts](#)
- [Enabling User Accounts](#)
- [Deleting User Accounts](#)

Searching Users



Note: As long as you do not need to update, activate, or deactivate a user account, you do not need privileges to search. However, you *must* have the scope over the organization that the target user belongs to. For example, a GA from one organization can search for users in another organization, *if* that organization is in their purview.

To search for users with the specified criteria:

1. Ensure that you are logged in with the appropriate scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 14-1.)

Figure 14-1 Search Users and Administrators Page

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title "Arcot Administration Console" is in the center. On the right, a user is logged in as "BLAURIE (DEFAULTORG)" with a "Logout" link and a timestamp "Last Login Time 07/12/2010 11:16:24 GMT". Below the header, there are four tabs: "Users and Administrators" (selected), "Organizations", "Reports", and "Case Management". Under the "Users and Administrators" tab, there is a sub-section "Manage Users and Administrators" with two links: "Create Administrator" and "Search Users and Administrators" (highlighted with a green dot). The main content area is titled "Search Users and Administrators" and contains a text box with instructions: "Specify the search criteria to display the list of users. Use the Advanced Search link to additionally search on Status or Role. Tip: You need not enter the complete values in the fields. Also, you can specify the organization's Display Name to search for the user in an organization." Below this text box is a search form with five input fields labeled "First Name", "Last Name", "User Name", "Organization", and "Email". To the right of these fields are two buttons: "Search" and "Advanced Search".

4. Specify the search criteria to display the list of users. You can:
 - Search for users by specifying the partial or complete information of the user in the fields on this page.
 - Search for users by specifying the organization's Display Name.
 - Search for users by not specifying any criteria and just clicking **Search**.
 - Click the **Advanced Search** link to display the Advanced Search page (Figure 14-2) to search for users by specifying their Status or Role.

Figure 14-2 Advanced Search Page

Arcot Administration Console

Welcome [RLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Advanced Search

Click the User Search Criteria tab to specify the type of credential you want to base your search on.

User Search Criteria

User Details

First Name:

Middle Name:

Last Name:

User Name:

Organization:

Email Address:

User Status

Include Active Users: ☒

Include Inactive Users: ☐

Include Deleted Users: ☐

Available Roles

Role:

User
Customer Service Rep(CSR)
Fraud Analyst
Global Administrator

5. Specify the required details of the users and click **Search**.

A list of users matching the search criteria appears.

Updating User Information



Note: To be able to update a user account's settings, you must ensure that you have the appropriate privileges and scope to do so. MA can update any user account. GAs can update all user accounts in their scope. The OAs and UAs can update the user accounts in their purview.

To update a user's basic details (such as first, middle, and last names, contact information):

1. Ensure that you are logged in with the required privileges and scope to update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page ([Figure 14-1.](#))
4. Enter the partial or complete information of the user whose account you want to update (as discussed in the preceding section) and click **Search**.

A list of administrators matching the search criteria appears.

5. Click the *<user name>* link of the user whose account you want to edit.

The Basic User Information page similar to [Figure 14-3](#) appears.

Figure 14-3 Basic User Information Page

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo is on the left, and the title "Arcot Administration Console" is in the center. On the right, a welcome message reads "Welcome [RLAURIE \(DEFAULTORG\)](#) | [Logout](#)" with "Last Login Time 07/12/2010 11:16:24 GMT" below it. A navigation bar contains four tabs: "Users and Administrators" (selected), "Organizations", "Reports", and "Case Management". Below this, a sub-tab "Manage Users and Administrators" is active. The left sidebar lists "Manage Users and Administrators" with sub-links "Create Administrator" and "Search Users and Administrators". Under "Basic User Information", "User Details" is selected and highlighted with a green dot. The main content area shows a summary box with "User Name: PETER", "Organization: DEFAULT ORGANIZATION", and "Status: Active". Below this is a "Basic User Information" tab. A "User Information" box contains the following details: First Name: FNAME, Middle Name: N/A, Last Name: LNAME, Email Address: user@arcot.com, Creation Date: 07/09/2010 09:16:02 GMT, Last Modified: 07/09/2010 09:16:02 GMT, and Phone Number: N/A. At the bottom of this box are "Edit" and "Return to Search" buttons.

Arcot Administration Console

Welcome [RLAURIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- User Details**

User Name: PETER **Organization: DEFAULT ORGANIZATION** **Status: Active**

Basic User Information

User Information

First Name: FNAME
Middle Name: N/A
Last Name: LNAME
Email Address: user@arcot.com
Creation Date: 07/09/2010 09:16:02 GMT
Last Modified: 07/09/2010 09:16:02 GMT
Phone Number: N/A

[Edit](#) [Return to Search](#)

- Click **Edit** to change the user information on this page, as shown in [Figure 14-4](#).

Figure 14-4 User Information Page

Arcot Administration Console

Welcome **PLAURIE** (DEFAULT ORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- **User Details**

User Name: PETER **Organization:** DEFAULT ORGANIZATION **Status:** Active

Basic User Information

User Information

Edit the required user information. Click the Next button to reset their password and the scope of management, if this user belongs to an administrative role.

Administrator Details

Date Created: 07/09/2010 09:16:02 GMT
Last Modified: 07/09/2010 09:16:02 GMT
First Name:
Middle Name:
Last Name:
Email Address:
Phone Number:

7. Edit the required fields (**First Name**, **Middle Name**, **Last Name**, **Email Address**, and **Phone Number**.)
8. Click **Save** to save the changes made and return to the User Information page.

Promoting Users to Administrators



Note: To be able to promote a user to an administrator, you must ensure that you have the appropriate privileges and scope to do so. MA can promote any user. GAs, OAs, and UAs can promote the users in their scope.

To update a user's administrative role, password, and management scope:

1. Ensure that you are logged in with the required privileges and scope to create administrators and update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 14-1.)
4. Enter the partial or complete information of the user whose account you want to update (as discussed in the preceding section) and click **Search**.

A list of users matching the search criteria appears.

5. Click the `<user name>` link of the user whose account you want to edit.
The Basic User Information page similar to Figure 14-3 appears.
6. Click **Edit** to open the editable User Information page (similar to Figure 14-4.)
7. If the user's **Email Address** is not specified, enter the same. This attribute is mandatory for administrators.
8. Click **Promote as Administrator** to display the Create Administrator page (Figure 14-5.)

Figure 14-5 Create Administrator Page

Arcot Administration Console

Welcome [PLAUBIE \(DEFAULTORG\)](#) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- [Search Users and Administrators](#)

Basic User Information

- User Details**

User Name: PETER **Organization:** DEFAULT ORGANIZATION **Status:** Active

Basic User Information

Create Administrator

Set the Administrator's Role, Scope, and Password credential.
Note: To reset the credential, the target administrator will need to go through the reset flow.

Role

Role: *

Set Password

Password: *

Confirm Password: *

Manages

All Organizations: ☐

Available Organizations

- DEFAULT ORGANIZA
- HSBC
- Safe Bank

Selected Organizations

9. On this page:

- Specify the role of the new administrator from the **Role** drop-down list.

- Enter the password for the administrator account in the **Password** and **Confirm Password** fields.
- In the **Manages** section, select the organizations that the administrator will have scope on:
 - Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.
 - or
 - Select the required organizations from the **Available Organizations** list and click the **>** button to add these organization to the **Selected Organizations** list.

The **Available Organizations** list displays *all* the organizations that are available in the scope of the logged in administrator. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.

10. Click **Create** to save the changes and create and activate the administrator account.

Disabling User Accounts

To prevent a user from logging in to their account for security reasons, you can disable their account instead of deleting it. If you disable user account, then they are locked out of their account, and cannot log in unless the account is re-enabled again.



Note: To be able to disable a user account, you must ensure that you have the appropriate privileges and scope to do so. MA can disable any user account, while GAs can disable all user accounts (including other GAs) within their scope. The OAs and UAs can disable all user accounts in their purview.

To disable a user account:

1. Ensure that you are logged in with the required privileges and scope to disable the user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page ([Figure 14-1.](#))
4. Enter the partial or complete information of the user whose account you want to disable and click **Search**.

You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (GA, OA, or UA).

The Search Results page (Figure 14-6) appears, with all the matches for the specified criteria.

Figure 14-6 Search Results

Welcome **RLAURIE** (DEFAULTORG) | [Logout](#)
Last Login Time 07/12/2010 11:16:24 GMT

Arcot Administration Console

Users and Administrators | Organizations | Reports | Case Management

Manage Users and Administrators

Manage Users and Administrators

- [Create Administrator](#)
- **Search Users and Administrators**

Search Results

Click the [User Name](#) link to view or edit the details. To enable, disable, or delete multiple user accounts, select the users and click the applicable button.
Note: You can also reorder the user list by clicking the [User Name](#) column heading.

First Name Last Name User Name Organization Email

[Advanced Search](#)

Select Users to Modify ◀◀ 1 2 ▶▶

☐	User Name	Full Name	Organization	Email	Role	User Status
☒	FRANK	FNAME LNAME	DEFAULT ORGANIZATION	user@arcot.com	User	Active
☐	LWARD	Lauren Ward	DEFAULT ORGANIZATION	lward@arcot.com	Organization Adminis...	Active

Results 11-12 of 12

5. Select one or more users whose accounts you want to disable.
6. Click **Disable** to disable the selected user account.

Enabling User Accounts

You might need to enable a disabled account. For example, you might disable an administrator account in case the administrator is on long vacation. This helps to prevent unauthorized access to that administrator's account.

You cannot search directly for disabled accounts by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You must perform an **Advanced Search** for such users and use the **Include Inactive Users** option to search.



Note: To be able to enable a user account, you must ensure that you have the appropriate privileges and scope to do so. MA can enable any account, while GAs can enable all accounts within their scope. The OAs and UAs can enable all user accounts in their purview.

To enable a locked-out user account:

1. Ensure that you are logged in with the required privileges to enable the user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page ([Figure 14-1.](#))
4. Click the **Advanced Search** link to search for users based on their status (active or inactive).
The Advanced Search page ([Figure 14-2](#)) appears.
5. Enter the partial or complete information of the user in **User Account** section.
6. In the **User Status** section, select the **Include Inactive Users** option to search for all inactive user accounts.
7. Click **Search** to display the list of all users matching the search criteria.
8. Select the users whose account you want to enable.
9. Click **Enable** to enable the user accounts.

Deleting User Accounts

After a user account is deleted, all privileges associated with the account are permanently deleted. As a result, the user can no longer log in to your application. However, their account information and credentials *are not* removed from the system.

If you create a new user account with the same name as a previously deleted user, then the new account *does not* automatically assume the privileges of the previously deleted account. If you need to duplicate a deleted account, then you must manually re-create all privileges.



Note: To be able to delete a user account, you must ensure that you have the appropriate privileges and scope to do so. MA can delete any account, while GAs can delete all accounts (including other GAs), *except* the MA account, within their scope. The OAs and UAs can delete all user accounts in their purview.

To delete a user account:

1. Ensure that you are logged in with the required privileges to delete the user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page ([Figure 14-1.](#))
4. Enter the partial or complete information of the user whose account you want to delete and click **Search**.

You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (User).

The Search Results page (similar to [Figure 14-6](#)) appears, with all the matches for the specified criteria.

5. Select one or more users whose accounts you want to delete.
6. Click **Delete**.



Note: Even though you have deleted the user, their account information is still maintained in the database.

Chapter 15

Managing Cases



Important: In this chapter, some tasks ([Handling Cases](#)) can be performed by Customer Support Representatives, some ([Analyzing Transactions](#)) only by Fraud Analysts, and some ([Managing the Case Queue](#)) by Queue Managers. Between these three case roles, the tasks are mutually exclusive.

However, an Organization Administrator (OA) and a Global Administrator (GA) have all the privileges to handle these tasks for the organization(s) in their purview.

The Case Management feature of RiskFort provides your User Administrators (UAs) and Fraud Analysts (FAs) a single unified view of the data related to cases. This enables them to analyze the data more efficiently and take faster, better-informed decisions towards resolving the cases. In addition, Analysts can also constantly track the status and progress of their cases and maintain complete case histories with instant access to all related information.

This feature enables you to:

- Efficiently manage customer service and support
- Manage large numbers of cases and investigations
- Create actions and tasks with due dates
- Assign actions with due dates
- Record investigation notes and/or the resolution provided to the user
- Handle cases and tasks more efficiently
- Keep clear audit trail or history of actions on a case
- Analyze trends
- Generate fraud-related report

This chapter guides you through the basics of RiskFort Case Management, and covers the following topics:

- [Understanding RiskFort Cases](#)
- [Case Roles](#)
- [Case States](#)
- [Case Management Workflows](#)
- [Managing the Case Queue](#)
- [Analyzing Transactions](#)
- [Handling Cases](#)
- [Generating the Fraud Statistics Report](#)

Understanding RiskFort Cases

The *Case Management* feature enables you to investigate transactions, and intuitively and effectively manage the transactions that are marked suspicious. This feature simplifies the challenge of recording and documenting every phase of an investigation, creating a clear and comprehensive trail of activity. This feature also saves time by automatically creating a report of the findings, including a detailed listing of reason, recommendation, geolocation information, connection details, and risk assessment details.

This section explains the important points related to managed cases (or cases, in short) with the help of the following sections:

- [Case Basics](#)
- [Case Management Components](#)

Case Basics

The following is a gist of managed cases in RiskFort:

- All transactions (login, wire transfer, or any transaction that your application is evaluating risk for) for a user that result in the **Deny** or **Increase Authentication** advice in the RiskFort system are considered a *case*.
In other words, one case can comprise multiple suspicious transactions for a user.
- Every case provides information related to the user, transactions details, and case history.

In other words, there is a strict 1:1 mapping between a user and open cases. As a result if a case is already open for the user, then a new suspicious transaction is added to the existing case. A new case is *not* created if a user already has a case open.

- At any time, a user can only have one open case in the system.
- At any time, a view into the case from the Administration Console shows all the transactions within the case that have not been handled by an administrator and, therefore, their Fraud status is still undetermined.
- After a case is created in the system, it is not allowed to be closed as long as *all* the transactions within the case are not handled (marked as Fraud or Not A Fraud).

When a Customer Support Representative (CSR) handles all these transactions, they must close the case explicitly. Only then the case is considered to be closed.

- If a case is closed, then any new warnings or suspect transactions for a given user result in creation of a new case in the system. All new and future transactions are assigned to this new case.

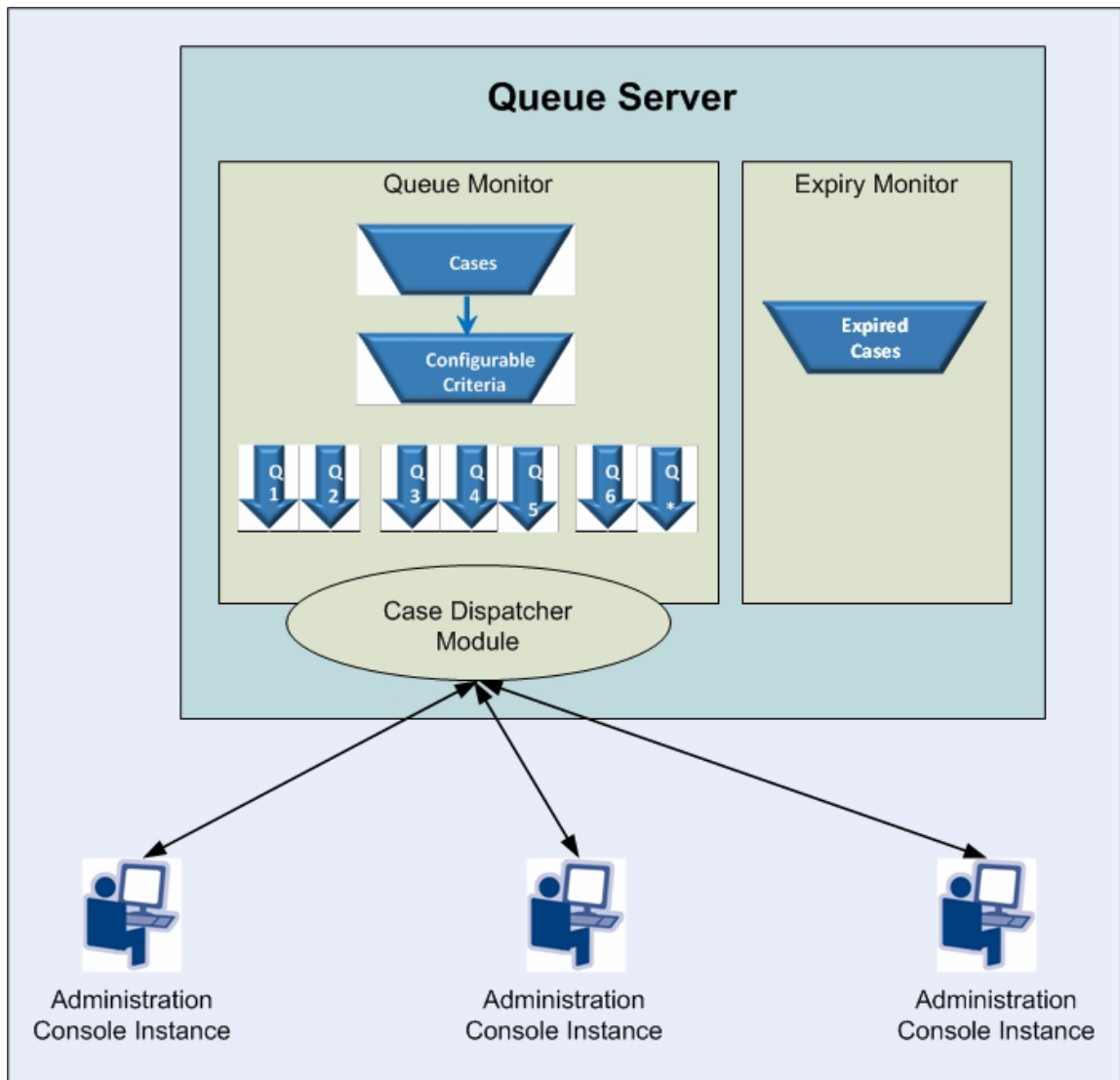
Case Management Components

The components of the Case Management module include:

- [Case Queues](#)
- [Queue Server](#)
- [Queue Monitor Thread](#)
- [Case Dispatcher Module](#)
- [Expiry Monitor Thread](#)

[Figure 15-1](#) illustrates how these components work together.

Figure 15-1 Case Management Components

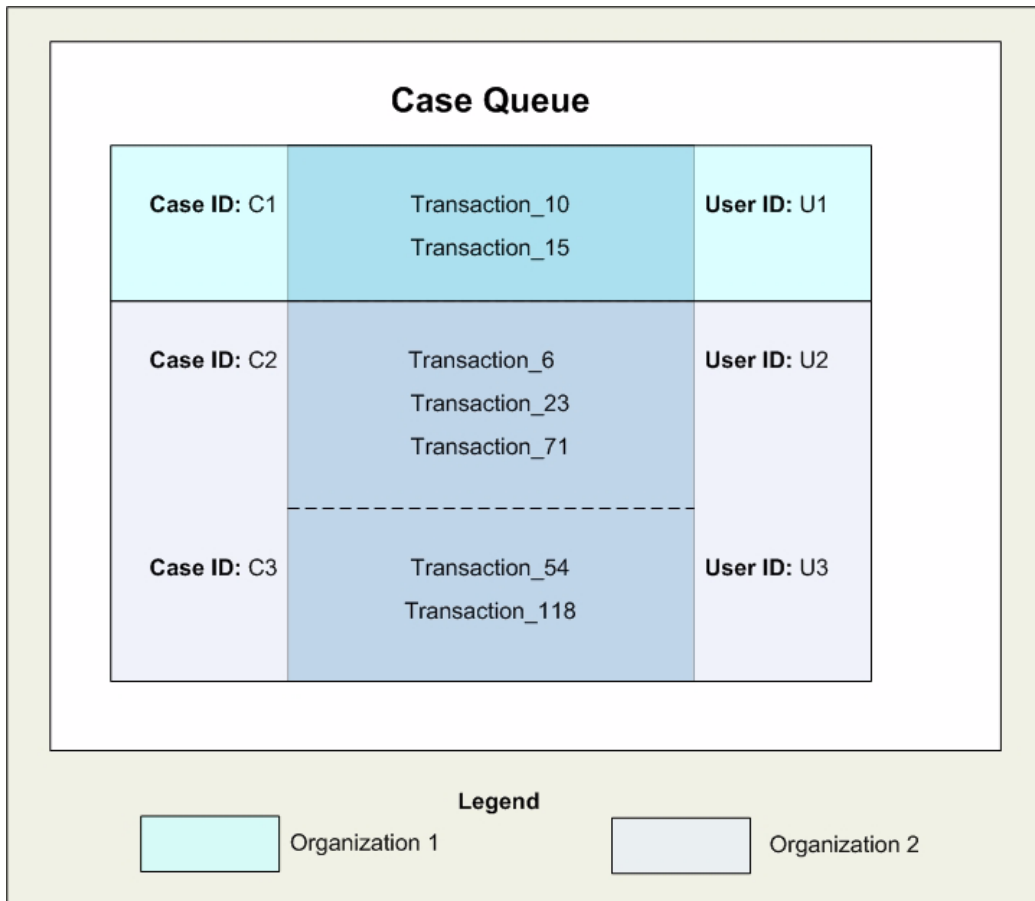


Case Queues

A *Case Queue* (or simply a *Queue*) is a list of cases that are grouped based on criteria, such as **Date Created**, **Date Updated**, **Number of Open Transactions**, and **Next Action Date**. Currently, RiskFort supports one Queue for each organization in the system.

Figure 15-2 depicts what a typical Queue looks like.

Figure 15-2 A Case Queue



Queues are managed by [Queue Managers](#), and are associated with a Queue Name, Case Order criteria in the Queue, and Case Priority. The [Queue Monitor Thread](#) looks at all the existing cases in the system that need to be worked on and assigns these cases to individual Queues, based on the respective Queue Criteria.

After the cases are assigned to individual Queues, the Queue Manager creates a Queue-to-CSR mapping. This mapping is then cached when the Case Management Queuing Server starts up and is subsequently used by the [Queue Server](#) for case allocation. [Customer Service Representatives](#) are allocated cases (through the Administration Console interface) to work on from their respective Queues.



Note: More than one CSRs can be allocated to a Queue in an organization. Also, if there are multiple organizations in a CSR's purview, the CSR can be allocated to multiple Queues.

Queue Server

The *Queue Server* is responsible for:

- Caching [Case Queues](#) and Queue-to-Administrator mapping with the help of the [Queue Monitor Thread](#).
- Dispatching the cases in the [Case Queues](#) to the active Administration Console instances with the help of [Case Dispatcher Module](#).
- Maintaining the updated list of expired cases with the help of [Expiry Monitor Thread](#).

Queue Monitor Thread

The *Queue Monitor* (sometimes referred to as *Scheduler*) thread runs at the [Queue Server](#)-end and is responsible for creating the Case Schedule, populating the [Case Queues](#) with cases, and readies the Queues for [Case Dispatcher Module](#).

This thread works as follows:

1. It wakes up at a pre-defined interval and fetches the list of all the latest cases from the database where:
 - At least one transaction shows the Fraud Status as **Undetermined**.

and

 - The case has not expired.
2. Caches the Queues with cases.
3. Based on the case state (see "[Case States](#)" on page 15-236 for more information) and other criteria (such as **Transaction Date**, **Transaction Amount**, or **Next Action Date**), it then assigns the cases into the [Case Queues](#).
4. When a case is assigned to the Queue, an in-memory list for the Queue is created.

5. On completion of the case assignment to a Queue, the state of all the assigned cases is changed to OPEN.
6. When the [Customer Service Representatives](#) (CSRs) click the **Save and Go to Next Case** or the **Go to Next Case** button:
 - a. A request to fetch the next case in the Queue is sent to the [Queue Monitor Thread](#) via [Queue Server](#).
 - b. In response, the [Case Dispatcher Module](#) picks the case from the memory queue and returns its `Case ID` to the Administration Console instance from where the request originated.
7. The state of the case is then changed to IN PROGRESS, and the CSRs can work on the case.
8. On receiving the `Case ID`, the Administration Console instance fetches all the transactions for the case from the database and displays the same to the CSR.

Based on the case review process, the case state can change. See section, [“Case States” on page 15-236](#) for more information.

Case Dispatcher Module

The *Case Dispatcher Module* (referred to as *Dispatcher*, in short) listens to the case requests from the individual [Customer Service Representatives](#) (CSRs) at the [Queue Server](#)-end and "pushes" the cases (as per their order in the Queue) from the [Case Queues](#) to the individual Administration Console instances on demand.

This module works as follows:

1. When CSR logs in, a request is sent to the Dispatcher to fetch the next case.
2. The Dispatcher fetches the next case from the Queue(s) assigned to this CSR
3. The Dispatcher, then, acquires lock on the selected case in the RiskFort database.
4. The Dispatcher also changes the status of the case from OPEN to INPROGRESS and updates the affected table with the name of the CSR from whose Administration Console instance the request originated.
5. The Dispatcher, then, sends the case details back to the Administration Console instance, which then fetches the transactions for the case and displays them on the screen for the CSR.
6. The Administration Console instance also sets a Timeout for the displayed case details.

This prevents the CSR from opening a case page and then not working on it within the pre-defined time interval. If the current case allocation to the CSR times out, an appropriate message is displayed to the CSR. The case subsequently times out and its status is changed OPEN.

7. If the currently displayed case does *not* timeout and the CSR moves to the next case (by clicking the **Go To Next Case** button on their screen) in the Queue, the case status is changed from INPROGRESS back to OPEN.

Expiry Monitor Thread

The *Expiry Monitor* thread is responsible for marking all the cases that have expired since the last time the thread ran. It wakes up at a much lesser frequency than the [Queue Monitor Thread](#).

This thread works as follows:

1. It wakes up at a pre-defined and configurable interval and fetches a list of all cases:
 - That are in the OPEN or NEW state.and
 - For which the case update time is more than the configured expiration time.

In other words, it looks for cases that have not been worked upon and for which no new alerts have been generated

2. Next, the thread updates the status of all cases identified in the preceding step as EXPIRED in the RiskFort database.
3. The thread goes back to sleep.

Case Roles

The Case Management feature supports the following broad categories of roles:

- [Customer Service Representatives](#)
- [Queue Managers](#)
- [Fraud Analysts](#)

Subsection, “[Case Role Privilege Summary](#)”, summarizes the privileges available to these roles.

Customer Service Representatives

As the name suggests, *Customer Support Representatives* (CSRs) are your organization's interface with the end user. They are responsible for:

- [Working on Cases](#)
- [Handling Customer Calls](#)

Working on Cases

They typically review cases that are automatically allocated to them and work on these cases. When they start working on a case, the case is marked with their name. As a result, the case will not show in another CSR's screen. However, the [Queue Managers](#) can "re-assign" the case to another CSR by assigning another CSR to the Queue.

They also call end users to confirm the authenticity of a suspect transaction. Their main activities include:

- If required, call the end users to verify if a transaction is fraudulent or not.
- Add users to the **Exception User List** for a specified duration, based on the user input.
The default duration is 10 days, but they can change it as required.
- After reviewing a case, they can "Update" the case. As a result of which, they can change the case status from **In Progress** to one of the following:
 - **On Hold**
 - **Closed**
- They can also take appropriate notes in a free-form field to capture the progress of the investigation.

Handling Customer Calls

At times, the CSRs also handle incoming calls from the end users. (In other words, they attend customer calls.) For example, a customer might call the Call Center because they see transactions that they did not perform. In such cases, these operators record the input from the customer, if a case for the specified user already exists. If a case does not exist for the customer, then a case is generated automatically.



Note: The input collected by CSRs is used by the Fraud Analyst for analyses.

In this case, the CSRs:

- Handle user calls.
- Record user inputs.
They can take appropriate notes in a free-form field to capture the progress of the investigation.
- View recent activities of the user.
- Add users to the **Exception User List** for a specified duration, based on the user input.
The default duration is 10 days, but they can change it as required.
- Search for the transactions by the user in the given time period.

Queue Managers

Queue Managers (or simply, Supervisors) determine the order in which cases are assigned to the Queue. They can:

- Manage the Queue for all organizations in their scope.
See section “[Case Queues](#)” on page 15-229, for more information on Queues.
- Assign and reassign CSRs to the Queues in their scope.



Note: By default, Queue Managers *cannot* perform the tasks of a Fraud Analyst. However, you can use **Custom Roles** to create a new role based on Queue Manager and assign the FA prelates to this role.

See “[Creating a Custom Role](#)” in [Chapter 3](#) for more information on how to create Custom Roles.

Fraud Analysts

Fraud Analysts (FAs) research and analyze fraud patterns in transactions to define anti-fraud strategies. They analyze the trends in transactions by using the truth data collected by other [Customer Service Representatives](#) and the available filters, such as:

- Transactions by the same user in the given time period.
- Transactions from the same user device in the given time period.
- Transactions from the same IP address in the given time period.

Based on their analyses, FAs can then advise the system administrators on fine-tuning RiskFort. In addition, if they suspect a transaction to be suspicious, they can raise a request for [Customer Service Representatives](#) to call the end user and find more details related to the suspect transactions, even if the system had not suspected those transactions previously.

The following list describes the main functions performed by Fraud Analysts:

- They can log in and view the list of transactions in real time.
- They can set a combination of filter conditions to view transactions for all users over a period of time for those matching specific risk status values.
- As part of the investigation, the FA can also search for the similar transactions. They can define the filter to detect similarity based on:
 - Transactions by the same user in the given time period.
 - Transactions from the same user device in the given time period.
 - Transactions from the same IP address in the given time period.
- If the transaction set is large, they can also export the data offline and then analyze it.
- If they locate suspicious patterns, they can raise alerts on those transactions for further investigation by the CSRs. The "alerted" transactions are automatically added to the case for the user in question.



Note: Fraud Analysts *cannot* update any cases.

Case Role Privilege Summary

[Table 15-1](#) summarizes the privileges available to the case roles discussed in the preceding sections.

Table 15-1. Case Role Privilege Summary

Privilege	CSR	Queue Manager	Fraud Analyst
View Cases	✓	--	--
Search Cases	✓	--	--
Update Cases	✓	--	--
Filter Cases	✓	--	--

Table 15-1. Case Role Privilege Summary

Privilege	CSR	Queue Manager	Fraud Analyst
Add User to Exception User List	✓	--	--
Manage Queues (See for more information on Queues)	--	✓	--
View Transactions	--	--	✓
Filter and Search Transactions	--	--	✓
Add Transactions to Cases (Raise Alerts)	✓	--	✓
Analyze Transactions	--	--	✓
Export Transaction Data Offline	--	--	✓

Case States

During its lifecycle, a case can progress through the following states:

- [New](#)
- [Open](#)
- [In Progress](#)
- [On Hold](#)
- [Expired](#)
- [Closed](#)

New

When a user transaction results in **Increase Authentication** or **Deny** advice, then a new case is created for the user, if a corresponding case does not already exist.

The case remains in the **New** state until a Customer Service Representative (CSR) opens it or the case expires.

Open

When a Customer Service Representative (CSR) opens a new case assigned to them, the case is activated and its state changes to **Open**. When a case is in the **Open** state, new transactions or events can be added to the case.

Unless the case state is either **On Hold** or **Closed**, every case remains in the **Open** state.

In Progress

While a Customer Service Representative (CSR) is working on a case, the case state remains **In Progress**. In other words, when they click the **Cancel** button for the current case or click the **Go To Next Case** button to move to the next case assigned to them, the currently open case state changes to **Open**, or to the state that they explicitly changed the case to.



Note: Both Customer Service Representative (CSR) can change a case in **On Hold** state to **In Progress** state.

On Hold

When a Customer Service Representative (CSR) postpones the further investigation of a case by specifying the **Next Action Date** for an **In Progress** case, then the case state changes to **On Hold**.



Note: All events that are generated within the timeframe of **Next Action Date** are appended to case.

When the specified **Next Action Date** arrives, the case state automatically changes to **Open**.

Expired

When no Customer Service Representative (CSR) works on a **New** case within a pre-defined number of days, the case state changes to **Expired**.



Note: The time the last transaction was added to the case or was updated is considered as the *Starting Date* for the case. The case *Expiration Date* is calculated as the *Starting Date* + N days, where N is a configurable value. The default value for N is **10 days**.

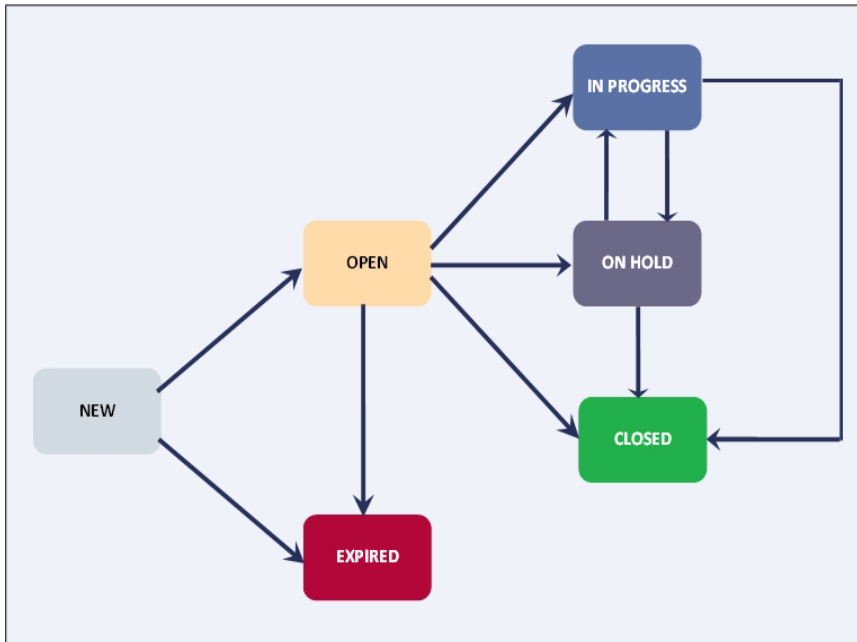
New transactions cannot be added to an expired case. A new case (and therefore a new **Case ID**) is created and the new transactions or events are added to this new case.

Closed

When a Customer Service Representative (CSR) resolves an Open case and explicitly marks it as **Closed**, then the case state changes to **Closed**.

Figure 15-3 illustrates how the states of a case change.

Figure 15-3 Case States



Case State Permissions At a Glance

Table 15-2 summarizes the case state manipulation privileges available to the case roles discussed in the preceding sections.

Table 15-2. Case State Change Permission Summary

Case State	Case Operators		Fraud Analyst
	CSR	Queue Manager	
New	--	--	--
Open	✓	--	--
In Progress	--	--	--

Table 15-2. Case State Change Permission Summary

Case State	Case Operators		Fraud Analyst
	CSR	Queue Manager	
On Hold	✓	--	--
Expired	--	--	--
Closed	✓	--	--

Case Management Workflows

This section covers the workflows for the following phases in a case's lifecycle:

1. [Case Generation](#)
2. [Case Queuing](#)
3. [Case Assignment](#)
4. [Case Handling](#)
5. [Case Expiry](#)
6. [Fraud Analysis](#)

Case Generation

Typically, cases are created automatically by the system. However, if a case operator manually flags a suspicious transaction for a user or a Fraud Analyst discovers a suspicious pattern in user transactions, then they can add the suspicious transactions to the case.

A case is generated when:

- The advice for the risk evaluation for a transaction is either **Increase Authentication** or **Deny**.



Note: If a case is already open for the user, then this transaction is added to the existing case.

- A user contacts your Call Center to dispute a transaction.

In this case, the case operator can either refer the disputed transactions for further investigation or can mark the transaction as a fraud. In both the cases, the transaction is automatically added to a case.

- A Fraud Analyst suspects some transactions to be fraudulent (typically, based on patterns detected earlier) and marks them for further investigation.



Note: These transactions are then added to the existing case.

Case Queuing

When a case is created and transactions are added to the case, the cases need to be assigned to the Queue that belongs to the organization. In addition, administrators (CSRs) who can work on these cases must also be assigned to each Queue. The [Queue Monitor Thread](#) plays the pivotal role in this case.

See [“Queue Monitor Thread” on page 15-230](#) for detailed information on how this thread queues cases.

Case Assignment

After a case has been queued, it then it then needs to be dispatched to each CSR’s screen. The [Case Dispatcher Module](#) plays the pivotal role in this case.

See [“Case Dispatcher Module” on page 15-231](#) for detailed information on how this thread dispatches cases.

Notes Related to Case Assignment

Some points to remember on this topic are:

- A new case is assigned to a CSR from the organization to which the case belongs.
- The cases are assigned based on their order in the Case Queue. The order criteria can include:
 - Next Contact/Action Date
 - Number of open transactions in the case
 - Age of the case (Date Created)
 - How long ago the case was last updated
- Every case is eventually handled by a CSR in an organization.

Case Handling

Cases are handled by the [Customer Service Representatives](#) (CSRs) as follows:

- A new transaction flagged by the FA or a Deny or Increase Authentication advice generated for a transaction creates a new case. The status of the case *before* the [Queue Monitor Thread](#) schedules it is **NEW**. The [Queue Monitor Thread](#) changes it to **OPEN**, and when a CSR finally views the case, the case status is changed to **INPROGRESS**.



Note: Even before the case is handled by a CSR, more flagged transactions might be added to the case.

- A CSR is automatically assigned to the work on the case.
- Contact the user out of band, say by sending an email or by calling them on the specified contact number.
- Based on the ongoing investigation and results of contacting the end user, the CSR can update the case, as it develops:
 - Search for transactions based on a specific time interval.
 - During the user interaction, add previously unsuspected transactions to the case.
 - Choose resolutions for one or more of the transactions in the case.
 - Mark the case for follow up and set the **Next Action Date**.
Typically, the Case Status of such cases is then updated to either INPROGRESS or ONHOLD, and the user is contacted by a CSR later.
- Based on user input, add the user to the **Exception User List** for a specified period of time.
- Resolve the case and change the **Case Status** to CLOSED.
- The [Queue Managers](#) can also reopen an expired case, if required.

Case Expiry

A case can expire if all of its transactions are not handled within the stipulated amount of time or if there is no activity on the case for a pre-defined time period.

See “[Expiry Monitor Thread](#)” on page 15-232 for detailed information on how this thread manages expired cases.

Fraud Analysis

The gist of the fraud analysis workflow for transactions by [Fraud Analysts](#) is as follows:

- FAs can search for transactions based on criteria such as, Transaction Date, Secondary Authentication Status, Transaction type, Risk Advice and Case Status (see “[Step 1: Viewing Transactions Summary](#)”):
 - All transactions are initially shown in the Transaction Summary view.
 - Initially, all transactions have the Case Status of **New**.
 - The list of transactions can be exported into a [.csv](#) file for processing in Microsoft Excel.
- The FAs can click a case to view its details. (See “[Step 2: Viewing Case Details](#)”.)
- The FAs can also search for all transactions that are similar to a case. (See “[Step 3: Viewing Similar Transactions](#)”.)
- If they find suspect transactions and potential fraud patterns during their analyses, FAs can mark the transactions for further investigations by CSRs. (See “[Step 4: Marking Transactions for Further Investigation](#)”.)

Managing the Case Queue



Important: Only an OA or a Queue Manager (QM) can perform the tasks (for the organizations that are in their scope) in this section. The MA, GAs, UAs, FAs, and CSRs *cannot* perform these tasks.

This section walks you through the following tasks related to Case Queue management:

- [Viewing the Status of the Queue](#)
- [Updating the Status of the Queue](#)

Viewing the Status of the Queue

By using the View Queue Status page, you can view the latest statistics (**Open Cases**, **In-Progress Cases**, **Total Cases**, and **Number of Administrators Assigned**) related to the **DEFAULT** Queue. It also shows the details of the **Cases Handled in the Last 8 Hours**.

To view the Queue Status:

1. Log in as an OA or a QM.

2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **View Queue Status** link to display the corresponding page.

Figure 15-4 The View Queue Status Page



4. Specify the Organization whose Queue Status you want to see from the **Select Organization** list.

The updated page (Figure 15-5) with the updated Queue details appears.

Figure 15-5 The View Queue Status Page

Arcot Administration Console

Welcome **PRUSH (DEFAULT.TORG)** | [Logout](#)
Last Login Time 07/12/2010 05:34:38 GMT

Case Management

Case Management

Queue Management

- View Queue Status
- Manage Queues

Select Organization: **DEFAULT ORGANIZATION**

Queue Status

This report gives current status of the queue.

Queue Name	Open Cases	In-Progress Cases	Total Cases	No. of Administrators Assigned
DEFAULT	6	0	6	0

Cases Handled in Last 8 Hours

This report gives information for last 8 hours.

Duration	Inbound Cases	Outbound Cases	Total Number of Cases Handled
Last 1 hour	0	0	0
Last 2 hour	0	0	0
Last 3 hour	0	0	0
Last 4 hour	0	0	0
Last 5 hour	0	0	0
Last 6 hour	0	0	0
Last 7 hour	0	0	0
Last 8 hour	0	0	0

Updating the Status of the Queue

You can update the status of the **DEFAULT** Queue by using any one of the following methods:

- By clicking the **View Queue Status** link to display the corresponding page, and then clicking the **DEFAULT** link in the **Queue Status** section, as discussed in the preceding section (“[Viewing the Status of the Queue](#)” on page 15-242.)
- By using the **Update Queues** link under the **Queue Management** section.

To update the status of the **DEFAULT** Queue by using the latter option:

- Log in as an OA or a QM.

2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Update Queues** link to display the Update Queues page.
4. Specify the Organization whose Queue Status you want to update from the **Select Organization** list.

The updated page (shown in [Figure 15-6](#)) appears.

Figure 15-6 The Update Queues Status Page

Arcot Administration Console

Welcome **PRUSH (DEFAULTORG)** | [Logout](#)
Last Login Time

Case Management

Manage Queues

Assign administrators who will work on Cases. Use 'Order By' to change the order in which Cases are displayed to the Case Handlers. For the changes to take effect, refresh the **Case Management Queuing Server** Cache by running the **arrtadmin** tool.

Select Organization:

Queue Name:

Queue Description:

Assign Administrators:

Administrators		Selected Administrators
FANTONY (DEFAULTORG)	>	
JHUME (DEFAULTORG)	>>	
MPARKER (DEFAULTORG)	<	
RLAURIE (DEFAULTORG)	<<	

Order By:

Then By:

Then By:

Then By:

5. Specify the **Queue Description**, if required.
6. For **Assign Administrators**:

- a. From the **Administrators** list, select the required administrators that you want to assign to the queue.



Tip: To select more than one administrators, press the SHIFT key and click the required administrators.

- b. Click the > button to move the selected administrators to the **Selected Administrators** list.



Note: If you want to move all the **Administrators** to the **Selected Administrators** list, then click the >> button to do so.

7. For **Order By**:
 - a. Specify the element (**Next Contact Date**, **Date Created**, **Date Updated**, or **Number of Open Transactions**) by which you want to sort the Queue.
 - b. Specify the order (**Ascending** or **Descending**) by which you want to order the corresponding element.
8. Click **Save** to save the updates you made on the screen.
9. Restart the Case Management Queuing Server instance. See [“Refreshing or Shutting Down a Server Instance” in Chapter 4](#) for detailed information on how to do this.

Analyzing Transactions



Important: Only OAs and Fraud Analysts (FAs) can analyze the user transactions for the organizations that are in their scope. The MA, GAs, UAs, and CSRs *cannot* perform this task.

Analyzing transactions is a multi-step process that can involve:

- [Step 1: Viewing Transactions Summary](#)
- [Step 2: Viewing Case Details](#)
- [Step 3: Viewing Similar Transactions](#)

- [Step 4: Marking Transactions for Further Investigation](#)

While looking at all the transactions based on the criteria that you specified in the Transactions Summary page ([Figure 15-8](#)), if you locate one or more suspect transactions, then you can further look into the details of these transactions ([Step 2: Viewing Case Details](#)). You can further locate a pattern by viewing similar transactions ([Step 3: Viewing Similar Transactions](#)). After you have analyzed the details and discovered patterns, you can mark suspect transactions for further investigation by the CSRs ([Step 4: Marking Transactions for Further Investigation](#).)

Step 1: Viewing Transactions Summary

To view the Transactions Summary report, perform the following steps:

1. Ensure that you are logged in with proper credentials (OA or Fraud Analyst.)
2. Activate the **Case Management** tab in the main menu.
3. Under the **Case Management** section, click the **Analyze Transactions** link.
4. From the **Select Organization** list, select the organization whose data you want to filter in the report.

The Select Transactions page appears, as shown in [Figure 15-7](#).

Figure 15-7 The Select Transactions Page

Arcot Administration Console

Welcome **RGRAHAM (DEFAULTORG)** | [Logout](#)
Last Login Time 07/06/2010 14:54:47 GMT

Case Management

Case Management

- Analyze Transactions
- Fraud Statistics Report

Select Transactions

Select your filter criteria for viewing risk evaluations.

Select Organization: **DEFAULT ORGANIZATION**

User Name:

☒ Transaction Date From: 07/06/2010 To: 07/06/2010

☐ Last Transactions: **--Select--**

Risk Advice

- All Advice
- Allow
- Alert
- IncreaseAuth
- Deny

Secondary Authentication Status

- All Status
- Success
- Failure

Fraud Status

- All Status
- Undetermined
- Confirmed Fraud
- Not a Fraud

Matched Rule: **All Rules**

- If required, specify the **User Name** whose transactions you want to view.



Note: If you do not specify any **User Name**, then all the transactions for the specified **Organization** are displayed.

- To filter the transactions based on one of following criteria:
 - Either select the pre-defined date range based on which you want to filter the transaction data in the **Transaction Date From** and **To** fields.

or

 - Select the **Last Transactions** option and then select the time interval (in minutes) for which you want to see the latest transactions that were performed.
- From the **Risk Advice** list, select the advices based on which you would like to filter the data.

8. From the **Secondary Authentication Status** list, select the statuses based on which you would like to filter the data.
9. From the **Fraud Status** list, select the statuses based on which you would like to filter the data.
10. From the **Matched Rules** list, select the rule based on which you would like to filter the transaction data.



Note: If you want to see the transactions for all rules that matched, then ensure that the default **All. Rules** option is selected.

11. Click **Submit** to generate the Transactions Summary page (Figure 15-8.)

You can export the information directly to a CSV file by clicking the **Export** button.

Figure 15-8 Transaction Summary Page

Transactions Summary

From 07/01/2010 To 07/06/2010

Number of transactions matching the search criteria: 4

Click the corresponding Detail link to view the details of a transaction.

☐ Details	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐ detail	PENNY	Undetermined		10.150.1.255	USER_DEVICE_NOT_ASSOCIATE...	07/06/2010 06:37:40 GMT	IncreaseAuth	Success	360
☐ detail	PENNY	Undetermined		10.150.1.255	USER_DEVICE_NOT_ASSOCIATE...	07/06/2010 06:37:30 GMT	IncreaseAuth	Failure	358
☐ detail	MONICA	Undetermined		10.150.1.255	USER_DEVICE_ASSOCIATED_AN...	07/06/2010 06:37:17 GMT	Allow		356
☐ detail	MONICA	Confirmed Fraud		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353

Table 15-3 describes the fields listed in the Transactions Summary page.

Table 15-3. Transactions Summary Page Fields

Fields	Description
Details	
User Name	The name of the user performing the transaction.

Table 15-3. Transactions Summary Page Fields

Fields	Description
Fraud Status	The fraud status of the case. This field can have one of the following statuses: • Undetermined • Confirmed Fraud • Not a Fraud
Country	Based on the IP Address , the country from which the transaction was performed.
IP Address	The IP address of the system or device used for the purchase transaction.
Matched Rule	The rule that matched and for which RiskFort flagged the transaction as risky.
Transaction Date	The timestamp when the transaction was performed.
Risk Advice	The action (ALLOW , ALERT , DENY , OR INCREASE AUTHENTICATION) suggested by RiskFort after evaluating the Risk Score of the transaction.
Secondary Auth Status	If the Risk Advice was INCREASE AUTHENTICATION , then this column specifies the result of the additional authentication that your application returned as feedback to RiskFort.
Transaction ID	The unique ID generated for each user transaction.

Step 2: Viewing Case Details

The Transactions Summary page can also be used to view details of any specific transaction or case. To view details of a specific case:

1. In the Transactions Summary page ([Figure 15-8](#)), click the required **details** link in the corresponding **Details** column.

The transaction details, as shown in [Figure 15-9](#), are displayed on the page. This page lists the details of the selected transaction, and also allows you to further filter transactions on the basis of available parameters ([Table 15-4](#)).

Figure 15-9 The Transaction Details

Basic Transaction Details			
Transaction ID:	356	Transaction Date:	07/06/2010 06:37:17 GMT
Action:	Login	User Name:	MONICA
Fraud Status:	Undetermined	Risk Advice:	Allow
Matched Rule:	USER_DEVICE_ASSOCIATED_AND_DEVICE_MFP_MATCHED Secondary Auth Status:		
Location Details			
IP Address:	10.150.1.255	City:	
State:		Country:	
Connection Type:		Line Speed:	
IP Routing Type:		Anonymizer Type:	
Risk Assessment Details			
User Known:	YES	Exception User:	NO
Device ID Matched:	YES	User Velocity Exceeded:	NO
User-Device Associated:	YES	Device Velocity Exceeded:	NO
Machine FingerPrint (MFP) Matched:	YES	Zone Hopped:	Not Available
MFP Match %:	80.0	Evaluation Callout Matched:	Not Available
Trusted IP:	NO	Negative IP:	NO
Trusted Aggregator:	NO	Negative Country:	Not Available

Table 15-4 describes the fields listed in the Transaction Details page.

Table 15-4. Transaction Details Page Fields

Fields	Description
Basic Transaction Details	
Transaction ID	The unique identifier of the transaction.
Transaction Date	The timestamp when the transaction was performed.
Action	The type of transaction performed by the user, which can be: • Login • Wire Transfer • Any other value that you specify through your application
User Name	The name of the user who performed the transaction.

Table 15-4. Transaction Details Page Fields

Fields	Description
Fraud Status	The current status of the fraud. Possible values are: • Under investigation • Not a Fraud • Fraud
Risk Advice	An action (ALLOW, ALERT, DENY, INCREASEAUTH) suggested by the Risk Assessment module after evaluating the risk score of the selected transaction.
Matched Rule	The rule that matched and for which RiskFort flagged the transaction as risky.
Secondary Authentication Status	If the Risk Advice was INCREASE AUTHENTICATION , then this column specifies the result of the additional authentication that your application returned as feedback to RiskFort.
Location Details	
IP Address	The IP address of the system or device used for the purchase transaction.
City	The city where the transaction was performed by the user.
State	The state to which the user belongs.
Country	The country to which the user belongs.
Connection Type	The connection type between the user's device and their Internet Service Provider. The possible values are: • Satellite • OCX • Frame Relay • TX • Dialup • Cable • DSL • ISDN • Fixed Wireless • Mobile Wireless
Line Speed	The speed of the user's internet connection. This is based on the Connection Type .

Table 15-4. Transaction Details Page Fields

Fields	Description
IP Routing Type	The IP routing method used for the connection. The possible values are: • Fixed (Cable, DSL, OCX) • AOL (AOL users) • POP (Dial up to regional ISP) • Super POP (Dial up to multi-state ISP) • Cache Proxy (Accelerator proxy, content distribution service) • Regional Proxy (Proxy for multiple states in a country) • Anonymizer (Anonymizing proxy) • Satellite (Consumer satellite or backbone satellite ISP) • International Proxy (Proxy funneling international traffic) • Mobile Gateway (Mobile device gateway to Internet) • Unknown (Cannot currently be determined)
Anonymizer Type	The type of anonymizer, if any, used for the connection. The possible values are: • Private (Anonymous proxies that are not publicly accessible. Typically belong to commercial ventures.) • Active (Anonymous proxies that tested positive within the last six months.) • Suspect (Anonymous proxies that tested positive within the last two years, but not the last six months.) • Inactive (Anonymous proxies that did not test positive in the last two years.) • Unknown (Anonymous proxies for which no positive test results are currently available.)
Risk Assessment Details	
User Known	Whether the User Known rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
Exception User	Whether the Exception User rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
Device ID Matched	Whether the Device-ID rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.

Table 15-4. Transaction Details Page Fields

Fields	Description
User Velocity Exceeded	Whether the User Velocity Check rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
User-Device Associated	Whether the User-Device Association was found in the RiskFort database. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
Device Velocity Exceeded	Whether the Device Velocity Check rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
Machine FingerPrint (MFP) Matched	Whether the MFP rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
Zone Hopped	Whether the Zone Hopping Check rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
MFP Match %	The match percentage of the incoming Machine FingerPrint (MFP) with the value stored in the RiskFort database. This is a numeric value.
Trusted IP	Whether the Trusted IP rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
Negative IP	Whether the Negative IP rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.

Table 15-4. Transaction Details Page Fields

Fields	Description
Trusted Aggregator	Whether the Trusted Aggregator rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.
Negative Country	Whether the Negative Country rule matched. The possible values are: • Yes: If the rule matched. • No: If the rule did not match. • N/A: If the information was not available during risk evaluation.

Step 3: Viewing Similar Transactions

The small table at the end of the transaction details ([Figure 15-10](#)) enables you to specify filter criteria to extract more fine-grained data for similar transactions from the RiskFort database.

Figure 15-10 Show Related Transactions Table

Show Related Transactions For: ☐ Same User Name ☐ Same Device ID ☐ Same IP Address
☒ Transaction Date From: 07/01/2010 [calendar] Hrs [dropdown] Mins [dropdown] To: 07/06/2010 [calendar] Hrs [dropdown] Mins [dropdown]
☐ Last Transactions: --Select-- [dropdown]
 [Show]

As visible in [Figure 15-10](#), transactions can be further filtered on the basis of the following parameters:

- **Same User:** By selecting this option, you can extract all transactions that belongs to the same user whose data you are currently viewing.
- **Same Device ID:** By selecting this option, you can extract all transactions done by using the same device that is used for the current transaction details that you are viewing.
- **Same IP Address:** By selecting this option, you can extract all transactions that have the same IP address as the current transaction details that you are viewing.
- **Transaction Date:** By specifying a date range (using the **From** and **To** fields), you can further filter all transactions that were performed in the specified time period.

or

- **Last Transactions:** By selecting the required time interval (in minutes), you can further filter all the latest transactions that were performed in the specified interval.

Viewing Related Transactions

To view the related transactions:

1. In the Transaction Details page, select any one or all of the following options:
 - **Same User**
 - **Same Device ID**
 - **Same IP Address**
 2. Either:
 - a. Enter a date range in the **With Transaction Date From** and **To** fields.

or

 - b. Select the **Last Transactions** option and then select latest time interval for which you want to see the related transactions.
 3. Click **Show**.
- The Transactions Summary page (similar to [Figure 15-8](#)) appears, displaying the records that matched the criteria.

Step 4: Marking Transactions for Further Investigation

After you have analyzed the details of suspect transaction and/or discovered patterns, you can mark suspect transactions for further investigation by the CSRs. To do so:

1. Ensure that you are logged in with the required privileges (OA or Fraud Analyst.)
2. Display the Transactions Summary page, as discussed in [“Step 1: Viewing Transactions Summary” on page 15-247](#).
3. Review the transactions that are displayed based on the criteria that you specified.
See section [“Step 2: Viewing Case Details” on page 15-250](#).
4. If you want to display similar patterns, follow the steps in section [“Step 3: Viewing Similar Transactions” on page 15-255](#).
5. Scroll back to the Transactions Summary table.
6. Select the transactions that you suspect by selecting the check boxes corresponding to the transaction in the table.
7. Click the **Mark for Investigation** button to generate cases for the transactions you marked.
These cases will now appear in the case lists for the CSRs to work on.

Handling Cases



Important: Only OAs and Customer Support Representatives (CSRs) can work on cases that belong to the organizations that are in their scope. The MA, GAs, UAs, and FAs *cannot* perform these tasks.

This section walks you through the following tasks that are related to handling cases and direct interaction with end users:

- [Working on Cases \(CSRs\)](#)
- [Managing Inbound Customer Calls \(CSRs\)](#)

Working on Cases (CSRs)

When RiskFort marks a transaction as suspect or an FA marks a transaction for further investigation, the case *automatically* appears in the CSR's case list.

To work on the cases in your list:

1. Log in as a CSR.
2. Activate the **Case Management** tab.

As shown in [Figure 15-11](#), the first case (in the order of the priority assigned to your cases) appears.

Figure 15-11 The Case Page

Arcot Administration Console Welcome **JHUME (DEFAULTORG)**
Last Login Time 07/06/2010 15:25:52

[Users and Administrators](#)
[Organizations](#)
[Reports](#)
[Case Management](#)

Case Management

User Name: JOSHUA(DEFAULTORG) Next Action Date: 07/06/2010 15:24:33 GMT
 Case History:

None

Alerts on this case

☐	Mark Selected As	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	Undetermined		10.150.1.255		07/06/2010 15:24:37 GMT	IncreaseAuth	Success	38

From: 06/06/2010 To: 07/06/2010 [Show Transactions](#) [Hide Transactions](#)

Case Status: **INPROGRESS**
 Note: -- Select --
 Additional Note:

☐ Next Action Date: 07/06/2010 Hrs: 00 Mins: 00
☐ Add User to Exception List
 From: 07/06/2010 To: 07/16/2010
 Reason:

[Save](#)
[Save and Go To Next Case](#)
[Go To Next Case](#)
[Cancel](#)

The fields in the page are explained in [Table 15-5](#).

Table 15-5. Fields for Working on Cases

Field	Description
User Name	The name of the user who is calling in.
Next Action Date	The date when the user must be contacted the next time.

Table 15-5. Fields for Working on Cases

Field	Description
Case History	The latest case Notes and Additional Notes entered by the previous call handler. If you would like to review all the previous notes in this field, then click the More... link to do so.
Alerts on This Case	
Mark Selected As	The Fraud Status of the transaction. The possible values in this field are: • Undetermined • Confirmed Fraud • Not a Fraud If you have more than one alerted transactions that need your attention <i>and</i> after talking to the user you determine that all of their Fraud Status is the same (say Confirmed Fraud or Not a Fraud), then you can use this drop-down list to set the same in one action.
Fraud Status	Based on the previous entry in the Mark Selected As field, this field can have one of the following statuses: • Undetermined • Confirmed Fraud • Not a Fraud
Country	Based on the IP Address , the country from which the transaction was performed.
IP Address	The IP address of the system or device used for the user transaction.
Matched Rule	The rule that matched and for which RiskFort flagged the transaction as risky.
Transaction Date	The timestamp when the given transaction was performed.
Risk Advice	The action (ALLOW , ALERT , DENY , OR INCREASE AUTHENTICATION) suggested by RiskFort after evaluating the Risk Score of the given transaction.
Secondary Auth Status	If the Risk Advice was INCREASE AUTHENTICATION , then this column specifies the result of the additional authentication that your application returned as feedback to RiskFort.

Table 15-5. Fields for Working on Cases

Field	Description
Transaction ID	The unique system-generated identifier for the user transaction. Note: If required, you can click the Transaction ID to view its details. (See Figure 15-12 .)
From To	The pre-defined date range using which you want to filter the data.
Show Transactions	The button to display the alerted transactions based on the preceding From and To fields.
Hide Transactions	The button to hide the displayed alerted transactions.
Case Status	The current status of the case. The possible values are: • INPROGRESS • ONHOLD • CLOSED
Note	The pre-determined reason for the update.
Additional Note	Any additional information (in addition to the preceding Note) that describes the reason for the change in the case status or any of the fields before. Important: This field <i>cannot</i> accept more than 250 characters.
Next Action Date	The date when the user must be contacted the next time for additional follow-up.
Add User to Exception List	If based on user inputs, you want to temporarily exclude a user from risk evaluation for a specified time interval. For example, a user is travelling to a Negative Country and you do not want the user to be denied any transaction for the same. In this case, you can add the user to the Exception User List. If the user is found in the Exception User List, then by default RiskFort returns a low Score and the ALLOW advice for transactions originating from these users.

Table 15-5. Fields for Working on Cases

Field	Description
From	The date range for which you want the user to be exempted from RiskFort risk evaluation.
To	
Reason	The reason for which the user is being added to the Exception User List.

Figure 15-12 The Transaction Summary for the Case

Arcot Administration Console

Welcome **JHUME (DEFAULTORG)** | [Logout](#)
Last Login Time 07/06/2010 15:25:52 GMT

Users and Administrators | Organizations | Reports | **Case Management**

Case Management

Case Management

- Work On Cases
- Manage Inbound Calls

Transactions Summary

Click the corresponding Detail link to view the details of a transaction.

Basic Transaction Details			
Transaction ID:	38	Transaction Date:	07/06/2010 15:24:37 GMT
Action:	Login	User Name:	JOSHUA
Fraud Status:	Undetermined	Risk Advice:	IncreaseAuth
Matched Rule:		Secondary Auth Status:	Success

Location Details			
IP Address:	10.150.1.255	City:	
State:		Country:	
Connection Type:		Line Speed:	
IP Routing Type:		Anonymizer Type:	

Risk Assessment Details			
User Known:	YES	Exception User:	NO
Device ID Matched:	YES	User Velocity Exceeded:	NO
User-Device Associated:	NO	Device Velocity Exceeded:	NO
Machine FingerPrint (MFP) Matched:	YES	Zone Hopped:	Not Available
MFP Match %:	80.0	Evaluation Callout Matched:	Not Available
Trusted IP:	NO	Negative IP:	NO
Trusted Aggregator:	NO	Negative Country:	Not Available

[Back](#)

- Perform the required actions to capture the user inputs by using the fields explain in [Table 15-5](#).
- When done, click one of the following buttons on the page:
 - Save** to update your changes to the case.

- **Save and Go To Next Case** to update your changes to the case and go to the next case assigned to you.
- **Go To Next Case** to go to the next case assigned to you without saving the changes.
- **Cancel** to cancel any changes you just made on the page.

Managing Inbound Customer Calls (CSRs)

When an end user calls your Customer Support Center to dispute a transaction, then the attending CSR must use the **Manage Inbound Calls** page (Figure 15-13) to capture the information provided by the user and make the required changes to the case based on this information.

Figure 15-13 The Manage Inbound Calls Page

User Name: MONICA
Next Action Date:

None

Case History:

Alerts on this case

☐	Mark Selected As	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353

From: 06/06/2010 To: 07/06/2010

Show Transactions Hide Transactions

☐	Mark Selected As	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353
☐	Undetermined	MONICA	Undetermined		10.150.1.255	USER_DEVICE_ASSOCIATED_AN...	07/06/2010 06:37:17 GMT	Allow		356

Case Status: INPROGRESS
Note: -- Select --
Additional Note:

☐ Next Action Date: 07/06/2010 Hrs: 00 Mins: 00
☐ Add User to Exception List

From: 07/06/2010 To: 07/16/2010
Reason:

Save Cancel

To make the required changes to the case by using the Manage Inbound Calls page:

1. Log in as a CSR.

2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Manage Inbound Calls** link to display the Manage Inbound Calls page.
4. From the **Select Organization** list, select the required organization.

The updated Manage Inbound Calls page shown in [Figure 15-13](#) appears.

Figure 15-14 The Manage Inbound Calls Page

The screenshot displays the Arcot Administration Console interface. At the top, the Arcot logo and 'Arcot Administration Console' title are visible, along with a user welcome message 'Welcome JHUME (DEFAULTORG)' and a 'Logout' link. The navigation bar includes tabs for 'Users and Administrators', 'Organizations', 'Reports', and 'Case Management'. The 'Case Management' tab is active, showing a sidebar with 'Case Management' and 'Manage Inbound Calls' (highlighted with a green dot). The main content area is titled 'Manage Inbound Calls' with a subtitle 'Select your filter criteria for viewing risk evaluations.' Below the subtitle is a form containing a 'Select Organization:' dropdown menu (currently showing 'DEFAULT ORGANIZATION'), a 'User Name:' text input field, and a 'Submit' button.

5. Specify the **User Name** who is calling in and click **Submit**.

The Manage Inbound Calls page is refreshed with the specified user's case information, as shown in [Figure 15-15](#).

Figure 15-15 The Manage Inbound Calls Page with User Information

User Name: MONICA Next Action Date:

Case History:

None

Alerts on this case

	Mark Selected As	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353

From: 06/06/2010 To: 07/06/2010 [Show Transactions](#) [Hide Transactions](#)

	Mark Selected As	User Name	Fraud Status	Country	IP Address	Matched Rule	Transaction Date	Risk Advice	Secondary Auth Status	Transaction ID
☐	Undetermined	MONICA	Undetermined		10.150.1.255	DEVICEIDCHECK	07/06/2010 06:37:06 GMT	IncreaseAuth	Success	353
☐	Undetermined	MONICA	Undetermined		10.150.1.255	USER_DEVICE_ASSOCIATED_AN...	07/06/2010 06:37:17 GMT	Allow		356

Case Status:

Note:

Additional Note:

☐ Next Action Date: 07/06/2010 Hrs: 00 Mins: 00

☐ Add User to Exception List

From: 07/06/2010 To: 07/16/2010

Reason:

The fields in the page are explained in [Table 15-5](#).

- Perform the required actions to capture the user inputs by using the fields explain in [Table 15-5](#).
- When done, click **Save** to update your changes to the case.

If you do not want to save the changes you just made, click **Cancel**.

Generating the Fraud Statistics Report



Important: Only OAs and Fraud Analysts (FAs) can generate this report for the organizations that are in their scope. The MA, GAs, UAs, and CSRs *cannot* generate this report.

The Fraud Statistics report (Figure 15-17) displays the overall statistical data for each risk advice that RiskFort generates in the specified time period.

To generate the Fraud Statistics report:

1. Ensure that you are logged in with proper credentials (OA, or FA.)
2. Activate the **Case Management** tab in the main menu.
3. Under the **Case Management** section, click the **Fraud Statistics Report** link.

The Fraud Statistics Report page appears, as shown in Figure 15-16.

Figure 15-16 Fraud Statistics Report

Arcot Administration Console

Welcome **BGRAHAM**(DEFAULTORG) | [Logout](#)
Last Login Time 07/06/2010 15:04:57 GMT

Case Management

Fraud Statistics Report

Specify the criteria to generate the report.

Organization Name
DEFAULT ORGANIZATION

Date Range
Custom

From
07/06/2010

To
07/06/2010

Display Report

4. Select the required organizations for which you want to generate this report from the **Organization Name** list.

- Select the **Date Range** from the drop-down menu.

You can also select a pre-defined date range in the **From** and **To** fields.

- Click **Display Report** to view the generated report.

The Fraud Statistics Report, as shown in [Figure 15-17](#), appears.

Figure 15-17 Fraud Statistics Report

Fraud Statistics Report				
<i>This report displays the overall statistics for each Risk Advice generated by RiskFort that matched the criteria that you specified.</i>				
Export New Report				
Date Range: From: 01/01/2009 To: 07/06/2010				
Risk Advice	Fraud	Not a Fraud	Unknown	Total
Allow	0 (0%)	0 (0%)	1 (100%)	1
Increase Authentication	1 (33%)	0 (0%)	2 (67%)	3
Alert	0 (0%)	0 (0%)	0 (0%)	0
Deny	0 (0%)	0 (0%)	0 (0%)	0
Total	1 (25%)	0 (0%)	3 (75%)	4

The Fraud Statics report displays information related to the overall transaction risk, as explained in [Table 15-6](#).

Table 15-6. Fraud Statistics Report Fields

Parameter	Description
Risk Advice	Specifies the action suggested by the RiskFort after evaluating the risk of each transaction. The generated risk advice can be one of the following: • Allow • Increase Authentication • Alert • Deny
Fraud	Specifies the total number and percentage of all transactions that were reported by RiskFort as fraudulent.
Not a Fraud	Specifies the total number and percentage of all transactions that were not considered fraudulent by RiskFort.

Table 15-6. Fraud Statistics Report Fields

Parameter	Description
Unknown	Specifies the total number and percentage of all transactions for which RiskFort did not have sufficient data to generate a risk advice.
Total	Specifies the total for all transactions that were: • Fraud • Not a Fraud • Unknown

7. Click **Export** to save the report to a file or click **New Report** to generate a new report by specifying different criteria.

Chapter 16

Managing Reports

Based on your administrator level, reports enable you to instantly summarize and analyze the information in RiskFort database. For example, a report can tell a higher-level administrator which of their administrators accessed the system, at what time, and what activities did they perform. Section, [“Summary of Reports Available to All Administrators”](#) provides an at-a-glance summary of all reports that are available to the different administrators in a tabular format. The sections following [Table 16-1](#) explain these reports:

- [Administrator Reports](#)
- [RiskFort Reports](#)
- [Case Management Reports](#)

Reports available through the Administration Console are generated based on the parameters (or filters) that you specify. As a result, you can control the output of a report based on values that you set when you run the reports. The parameters that you can use to filter data include:

- Date Range
- Administrator Name
- Organizations
- User Name

Section, [“Generating Reports” on page 16-294](#) walks you through the generic process to generate activity reports for administrators and RiskFort-specific reports.

You can also export all generated reports to a local file. See section, [“Exporting Reports” on page 16-295](#) for instructions to do so.

Summary of Reports Available to All Administrators

Table 16-1 summarizes the reports in all categories (Administrator Reports, RiskFort Reports, and Case Management Reports) that are available to all administrators in the system. These reports are then covered in detail in the following sections.

Table 16-1. Report Available to All Administrators: At a Glance

Administrator	Report Category		
	Administrator Report	RiskFort Report	Case Management Report
Master Administrator	My Activity Report	--	--
	Administrator Activity Report		
	Organization Report		
Global Administrator	My Activity Report	Risk Evaluation Detail Activity Report	Fraud Statistics Report
	Administrator Activity Report	Risk Advice Summary Report	
	User Activity Report	Trusted IP/Aggregator Report	
	Organization Report	Negative IP Address Report	
		Negative Country Report	
		Exception User Report	
		Add-On Rules Report	
		Rules Data Report	
		Rules Data Classification Report	

Table 16-1. Report Available to All Administrators: At a Glance

Administrator	Report Category		
	Administrator Report	RiskFort Report	Case Management Report
Organization Administrator	My Activity Report	Risk Evaluation Detail Activity Report	Fraud Statistics Report
	Administrator Activity Report	Risk Advice Summary Report	
	User Activity Report	Trusted IP/Aggregator Report	
	Organization Report	Negative IP Address Report	
		Negative Country Report	
		Exception User Report	
		Add-On Rules Report	
		Rules Data Report	
		Rules Data Classification Report	
User Administrator	My Activity Report	Risk Evaluation Detail Activity Report	Fraud Statistics Report
	Administrator Activity Report	Risk Advice Summary Report	
	User Activity Report	Exception User Report	
Fraud Analyst	My Activity Report	--	Fraud Statistics Report
Customer Support Representative	My Activity Report	Exception User Report	--

The following sections explain these reports in detail.

Administrator Reports

All Administrator reports available in the system include:

- [My Activity Report](#)
- [Administrator Activity Report](#)
- [User Activity Report](#)
- [Organization Report](#)

My Activity Report

This report lists all operations performed by the administrator who is currently logged in and is generating the report related to the actions and operations they have performed so far.

Even though the logged in administrator can view their activities by using the [Administrator Activity Report](#), this report is provided separately because:

- An administrator might not have scope over the organization to which they belong. For example, administrator *Alan* belongs to organization *MyOrg* but has scope over *ScopeOrg*. In this case Alan cannot view his activities by using the Administrator Activity Report, because he does not have the required scope.
- Administrator Activity Report lists the activities of all the administrators whose user name completely or partially matches to that of the specified user name. Therefore, the administrator has to search all pages of the report to get their activity report. My Activity report solves this problem, because the report shows the activities of only the logged-in administrator.

[Figure 16-1](#) shows a sample of My Activity Report.

Figure 16-1 My Activity Report

My Activity Report

This report displays the activity of the logged in administrator.

ExportNew Report

Date Range:

From: 01/01/2009

To: 01/08/2010

Table 16-2 explains the fields of this report.

Table 16-2. My Activity Report Fields

Report Field	Description
Date	The date and time of the activity.
Administrator Name	The name of the administrator who is generating the report.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	The unique ID generated for each activity performed by the administrator.
Event Type	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Status	The status of the action taken: • Success - If the action was completed successfully. • Failure - If the administrator failed to complete the action.
Reason	The reason why the operation failed.
Target User	The name of the user whose attributes were administered by the administrator.

Table 16-2. My Activity Report Fields

Report Field	Description
Target Organization	The organization on which the activity was performed.
Component	The resource that was used to perform the task. The column values can be: • Administration Console • WebFort
Session ID	The session identifier of the Administration Console to which the administrator logged in.
Instance ID	The unique identifier for the Administration Console application instance, in case multiple instances of the application are running.

Administrator Activity Report

This report lists all activities performed by the specified administrator, or by the administrators who belong to the specified organizations, given that they are in scope of the administrator generating this report.

By using this report, you can filter the activities of a specific administrator or view the activities for all the administrators of a single organization or multiple organizations. This report includes information such as, administrator login and logout timestamps, organization search, administrator account updates, and related details.

[Figure 16-2](#) shows a sample Administrator Activity Audit Report.

Figure 16-2 Administrator Activity Report

Administrator Activity Report

This report displays the administrative activities performed using the Arcot Administration Console.

ExportNew Report

Date Range:From: 01/01/2009To: 01/08/2010

123456>>>

Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID
01/08/2010 13:54:20	MASTERADMIN	MASTERADMIN	1045	View Report: My Activity Repor...	Success	N/A	N/A	MASTERADMIN	Admin Console	DFCC647A7DEFB2F6AE6A0D1D6579D4...	1
01/08/2010 13:53:45	MASTERADMIN	MASTERADMIN	1043	Admin Login	Success	N/A	N/A	N/A	Admin Console	DFCC647A7DEFB2F6AE6A0D1D6579D4...	1
01/08/2010 13:53:35	GA1	DEFAULT ORGANIZATION	1041	Admin Logout	Success	N/A	N/A	N/A	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:41:23	GA1	DEFAULT ORGANIZATION	1039	View Report: Administrator Act...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:40:10	GA1	DEFAULT ORGANIZATION	1037	View Report: My Activity Repor...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:35:13	GA1	DEFAULT ORGANIZATION	1035	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:24:17	GA1	DEFAULT ORGANIZATION	1018	Admin Login	Success	N/A	N/A	N/A	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:24:13	GA1	DEFAULT ORGANIZATION	1017	Update Password	Success	N/A	N/A	N/A	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:23:44	MASTERADMIN	MASTERADMIN	1015	Admin Logout	Success	N/A	N/A	N/A	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1
01/08/2010 13:23:38	MASTERADMIN	MASTERADMIN	1014	Create Administrator	Success	N/A	GA1	DEFAULT ORGANIZATION	Admin Console	4AFC8BD3D01DDF15034F2265707C58...	1

123456>>>

The fields of this report are same as those of My Activity Report. See [Table 16-2](#) for more information on the field details.

User Activity Report

This report lists all activities performed on user attributes, which include creating users, updating users, setting PAM, deleting users, update user status, and authenticating users. The report contains details such as, user name, status of the user, type of operations performed, and also the IP address of the user system.

To generate this report, you must specify:

- The **Date Range**.
- (Optional) The **User Name**.
- The required **Organization Name**.

Figure 16-3 shows a sample User Activity Report.

Figure 16-3 User Activity Report

User Activity Report

This report displays the user activity in the system.

Events to Display

All Events

Export

New Report

Date Range:

From: 01/08/2009

To: 01/08/2010

<< <

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

>> >

Date	User Name	Event Type	Organization	Status	Transaction ID	Reason	Client IP Address	Caller ID
01/08/2010 14:01:44	UA1	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:D6BD2EF7C0F7873...	N/A	127.0.0.1	N/A
01/08/2010 14:01:12	OA1	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:D6BD2EF7C0F7873...	N/A	127.0.0.1	N/A
01/08/2010 13:25:08	GA1	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:D6BD2EF7C0F7873...	N/A	127.0.0.1	N/A
01/07/2010 16:42:30	961753102595826	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A
01/07/2010 16:38:46	871311873732775	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A
01/07/2010 16:38:42	395723421848553	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A
01/07/2010 16:37:14	877169446285705	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A
01/07/2010 16:35:56	194574794370722	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A
01/07/2010 16:34:38	848770808795672	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A
01/07/2010 16:30:16	207713997468285	Create User	DEFAULT ORGANIZATION	Success	uds-1-urn:uuid:A3FE8AEBF20D3EE...	N/A	127.0.0.1	N/A

<< <

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

>> >

Table 16-3 explains the fields of this report.

Table 16-3. User Activity Report Fields

Report Field	Description
Date	The date and time of the activity.
User Name	The name of the user for whom the activity was performed.
Event Type	The type of activity (such as, create, update, and delete user) performed by the administrator.
Organization	The organization name to which the user belongs.
Status	The status of the operation: • Success - If the operation was completed successfully. • Failure - If the user failed to complete the operation.
Transaction ID	The unique ID generated for every activity performed by the user.
Reason	The reason why the Operation failed.

Table 16-3. User Activity Report Fields

Report Field	Description
Client IP Address	The IP address of the end user's system.
Caller ID	The unique identifier set by the calling application. Note: The Caller ID can be blank, if the calling application did not set the value.

Organization Report

This report provides the details of all operations performed in a specified organization. Irrespective of any rules and configurations, this report displays *all* the activities in the organization under the administrator's purview.

To generate this report, you must specify:

- The **Date Range**.
- The **Organization Name**, if required.

[Figure 16-4](#) shows a sample Organization Report.

Figure 16-4 Organization Report

Organization Report											
This report displays the activity of the administrators on the selected organization.											
Export New Report											
Date Range: From: 01/08/2009 To: 01/08/2010											
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000											
Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID
01/08/2010 16:13:52	GA1	DEFAULT ORGANIZATION	1090	View Report: Organization Repo...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	507AB71B528834EC05F28EF6E19DFD...	1
01/08/2010 14:37:55	GA1	DEFAULT ORGANIZATION	1070	View Report: View Risk Advice ...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:37:55	GA1	DEFAULT ORGANIZATION	1068	View Report: View Risk Advice ...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:24:21	GA1	DEFAULT ORGANIZATION	1066	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:05:36	GA1	DEFAULT ORGANIZATION	1058	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 14:00:14	GA1	DEFAULT ORGANIZATION	1057	Create Administrator	Success	N/A	UA1	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 13:59:43	GA1	DEFAULT ORGANIZATION	1055	Create Administrator	Success	N/A	OA1	DEFAULT ORGANIZATION	Admin Console	F3C1F58173FC4F0784757488E2E1BD...	1
01/08/2010 13:41:23	GA1	DEFAULT ORGANIZATION	1039	View Report: Administrator Act...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:40:10	GA1	DEFAULT ORGANIZATION	1037	View Report: My Activity Repor...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1
01/08/2010 13:35:13	GA1	DEFAULT ORGANIZATION	1035	View Report: View Risk Evaluat...	Success	N/A	N/A	DEFAULT ORGANIZATION	Admin Console	E5C331394027F9C59D2355C0D5C338...	1

Table 16-4 explains the fields of this report.

Table 16-4. Organization Report Fields

Report Field	Description
Date	The date and time of the activity.
Administrator Name	The name of the administrator who performed the activity.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	The unique identifier generated for every activity performed by the administrator.
Event Type	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.

Table 16-4. Organization Report Fields

Report Field	Description
Status	The status of the action taken: • Success - If the action was completed successfully. • Failure - If the administrator failed to complete the action.
Reason	The reason why the Operation failed.
Target User	The name of the user whose attributes were administered by the administrator.
Target Organization	The organization to which the user belongs.
Component	The resource that was used to perform the task. The column values can be: • Administration Console (Admin Console) • RiskFort (RiskFortResourcePack)
Session ID	The session identifier for the Administration Console to which the administrator logged in.
Instance ID	The unique identifier for the Administration Console application instance, in case multiple instances of the application are running.

RiskFort Reports

All the RiskFort configuration-related reports available in the system include:

- [Risk Evaluation Detail Activity Report](#)
- [Risk Advice Summary Report](#)
- [Trusted IP/Aggregator Report](#)
- [Negative IP Address Report](#)
- [Negative Country Report](#)
- [Exception User Report](#)
- [Add-On Rules Report](#)
- [Rules Data Report](#)
- [Rules Data Classification Report](#)

Risk Evaluation Detail Activity Report

This report displays *all* transactions performed by the RiskFort Server.

To generate this report, you must specify:

- The **Date Range**.
- The **Organization Name**, if required.
- The **User Name**, if required.

Figure 16-5 displays a Risk Evaluation Detail Activity Report page.

Figure 16-5 Risk Evaluation Detail Activity Report

Risk Evaluation Detail Activity Report

This report displays the risk evaluation details for all user transactions that matched the criteria that you specified.

EqualNew Report

Date Range: From 01/08/2009To 01/08/2010

1234567891011121314151617181920>>>

Date	User Name	Organization	Event Type	Event Status	Risk Score	Risk Advice	Matched Rule	Secondary Authentication Result	Raised Action	Caller ID	Transaction ID	Session ID	Instance ID	Country	Client IP Address	HTTP DeviceID	Flash DeviceID	Outgoing DeviceID	Exception User	Negative IP Address	Negative Country	Trailed IP	Trailed Aggregate	User Known	Machine Fingerprint Match	User Velocity	Device Velocity	Zone Hopping	Evaluation Cutoff	User Associated with Device and Device MFP Matched	Device MFP Not User Not Associated with Device	User Associated with Device and Device MFP Matched	Device MFP Not User Not Associated with Device	Add On Rules Result
01/07/2009 18:44:17	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	635	1635	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	95	Increase Authentication	DEVICE_VELOCITY	Not Available	DEFAULT	LOON	NA	634	1634	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	Yes	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	95	Increase Authentication	DEVICE_VELOCITY	Not Available	DEFAULT	LOON	NA	633	1633	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	Yes	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	632	1632	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	631	1631	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	630	1630	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	629	1629	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	628	1628	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:42:59	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	627	1627	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA
01/07/2009 18:41:48	98175310259503	DEFAULTORG	Evaluate Risk	SUCCESS	10	Allow	USER_DEVICE_ASSOCIATED_AND_DEV...	Not Available	DEFAULT	LOON	NA	626	1626	1	NA	101501.74	NA	NA	Yes2log2imH5SLuVCh83imv8Bo...	No	No	No	No	No	Yes	Yes	No	No	NA	Yes	No	No	No	NA

Table 16-5 lists the information included in a Risk Evaluation Detail Activity.

Table 16-5. Risk Evaluation Detail Activity Report Fields

Fields	Description
Date	The timestamp when risk evaluation was done for the user.
User Name	The unique ID of the user who performed the risk-evaluation activity.
Organization	The organization to which the user belongs.

Table 16-5. Risk Evaluation Detail Activity Report Fields (continued)

Fields	Description
Event Type	The type of risk-evaluation activity that was performed by RiskFort Server. These activities include: • Evaluate Risk • Update Attributes • Create Associations • Delete Associations
Event Status	The status of the event action taken and can be: • Success - RiskFort was able to perform the risk evaluation activity successfully. • Failure - RiskFort was not able to perform the risk evaluation activity successfully.
Risk Score	The score generated for the given transaction.
Risk Advice	The advice generated by RiskFort, depending on the score generated. The advice can be: • Allow • Deny • Alert • Increase Authentication
Matched Rule	The rule that matched.
Secondary Authentication Result	The result of secondary authentication that was returned to RiskFort by your application, if the Risk Advice generated by RiskFort was "Increase Authentication".
Ruleset	The ruleset configured for the organization to which the user belongs.
Action	The corresponding action (for example, Login) that was performed for the current Event.
Caller ID	A unique identifier passed to the RiskFort APIs by your calling application. Note: NOTE: Caller ID can be blank, if your calling application does not set the value.
Transaction ID	The internal unique ID provided by RiskFort Server for each activity performed by it.
Session ID	The session identifier of the Administration Console to which the administrator logged in.
Instance ID	The unique identifier of every instance of RiskFort Server, in case multiple instances are deployed in an installation.

Table 16-5. Risk Evaluation Detail Activity Report Fields (continued)

Fields	Description
Country	The country where the transaction originated. Note: This is derived from the Client IP Address value.
Client IP Address	The IP address of the end user's system.
HTTP DeviceID	Whether the HTTP Device ID was found on the user's end system. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Flash DeviceID	Whether the Flash Device ID was found on the user's end system. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Outgoing DeviceID	The corresponding Device ID that was generated during the transaction, in case it is the first transaction from the end user's system.
Exception User	Whether the user is in Exception User List or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Negative IP Address	Whether the Negative IP rule was applied or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Negative Country	Whether the Negative Country rule was applied or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Trusted IP	Whether the Trusted IP rule was applied or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Trusted Aggregator	Whether the Trusted Aggregator IP rule was applied or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
User Known	Whether the User Known rule (if the user is enrolled with RiskFort or not) was applied. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Machine FingerPrint Match	Whether the Machine FingerPrint Check for the user passed or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
User Velocity	Whether the User Velocity Check for the user passed or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.

Table 16-5. Risk Evaluation Detail Activity Report Fields (continued)

Fields	Description
Device Velocity	Whether the Device Velocity Check for the user passed or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Zone Hopping	Whether the Zone Hopping Check for the user passed or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Evaluation Callout	Whether an Evaluation Callout is configured or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
User Associated with Device and Device-MFP Matched	Whether the User Associated with Device and Device-MFP Matched rule is configured or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Device-MFP Matched but User Not Associated with Device	Whether the Device-MFP Matched but User Not Associated with Device rule is configured or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
User Associated with Device but Device-MFP Does Not Match	Whether the User Associated with Device but Device-MFP Does Not Match rule is configured or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
User Not Associated with Device and Device-MFP Does Not Match	Whether the User Not Associated with Device and Device-MFP Does Not Match rule is configured or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.
Add-On Rules Result	Whether an Add-On Rule is configured or not. In case it was applied, then the result (Yes or No) indicates whether the rule returned a match or not.

Risk Advice Summary Report

The Advice Summary Report provides an overall summary of advices that were returned by the RiskFort over the specified period of time ([Table 16-6](#)). It also displays a separate table with the detailed summary of all the secondary authentication results ([Table 16-7](#)).



Note: RiskFort returns risk advice for every transaction attempted by the user. Depending on the advice sent by RiskFort, your application may allow the user to complete a transaction or deny the transaction.

To generate this report, you must specify:

- The **Date Range**.
- The **Organization Name**, if required.

[Figure 16-6](#) displays a Risk Advice Summary Report page.

Figure 16-6 Risk Advice Summary Report

Risk Advice Summary Report				
<i>This report displays the summary of all Risk Advices generated by RiskFort for the criteria that you specified.</i>				
Risk Advice		Total		
Allow		170		
Increase Authentication		101		
Alert		67		
Deny		30		
Total		368		

Secondary Authentication Results Summary				
<i>This report displays the summary of all Secondary Authentication results that your application returned to RiskFort, if the original Risk Advice was "Increase Authentication".</i>				
Result	Success	Failure	Unknown	Total
Count	65	4	32	101
%	64%	4%	32%	100%

Table 16-6 lists the information included in a RiskFort Advice Summary Report:

Table 16-6. Risk Advice Summary Report Fields

Fields	Description
Risk Advice	The advice given by RiskFort for every transaction: • Allow- Your application must allow the transaction to proceed. • Increase Authentication - Your application must perform a secondary or additional authentication (such as prompting for secret questions or OTP authentication) before proceeding any further with the transaction. • Alert- Your application must create the user in RiskFort database. • Deny- Your application must deny the transaction from proceeding any further.
Total	The total number of risk advices generated.

Table 16-7 lists the information included in a Secondary Authentication Results Summary Report:

Table 16-7. Secondary Authentication Results Summary Fields

Fields	Description
Result	The summary of results when RiskFort generated the Increase Authentication advice and your application prompted the user for an additional authentication.
Success	The count for all secondary authentication attempts that were successful.
Failure	The count for all failed secondary authentication attempts by the user.
Unknown	The count for all instances when the result of the secondary authentication was not forwarded by your application to RiskFort.
Total	The total number of secondary authentications performed, irrespective of the Result generated.

Trusted IP/Aggregator Report

This report displays the list of all trusted aggregators or trusted IP address ranges configured in the system. This report is available for both Proposed as well as Active data:

- [Trusted IP Report](#)
- [Trusted Aggregator Report](#)

Trusted IP Report

To generate this report, specify the following options:

- The required **Organization Name**.

- The required **Ruleset Name**.
- The **Status**, which can be **ACTIVE** or **PROPOSED**.
- The **Trusted IP** option from the **Trusted IP/Trusted Aggregator** field.

Figure 16-7 shows a sample Trusted IP Report.

Figure 16-7 Trusted IP Report

Trusted IP/Aggregator Report			
<i>This report displays the details for the Trusted IPs or Aggregators based on the criteria that you specified.</i>			
			Export New Report
Start IP Address	End IP Address	Mask	Date Added
5.0.0.1	5.0.0.10	N/A	12/31/2007 18:30:00
5.1.7.7	N/A	255.255.255.0	12/31/2007 18:30:00
71.0.0.10	71.0.0.20	N/A	12/31/2007 18:30:00
203.203.205.0	N/A	255.255.0.255	12/31/2007 18:30:00
72.0.0.10	72.0.0.10	N/A	12/31/2007 18:30:00
203.203.203.203	203.203.203.204	N/A	12/31/2007 18:30:00
203.203.204.0	203.203.204.1	N/A	12/31/2007 18:30:00
71.1.0.0	N/A	255.255.255.0	12/31/2007 18:30:00

Table 16-8 explains the columns that you see in Trusted IP Report:

Table 16-8. Trusted IP Address Report Fields

Field	Description
Start IP Address	The IP address of the trusted aggregator.
End IP Address	The last address, if IP address range is specified.
Mask	The subnet mask value of the trusted aggregator IP address.
Date Added	The date when the first aggregator device ID was created.

Trusted Aggregator Report

To generate this report, specify the following options:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Status**, which can be **ACTIVE** or **PROPOSED**.
- The **Trusted Aggregator** option from the **Trusted IP/Trusted Aggregator** field.

Figure 16-8 shows a sample Trusted Aggregator Report.

Figure 16-8 Trusted Aggregator Report

Trusted IP/Aggregator Report										
<i>This report displays the details for the Trusted IPs or Aggregators based on the criteria that you specified.</i>										
Export New Report										
Aggregator Name	Start IP Address	End IP Address	Mask	Date Added	Aggregator ID 1	Date Created	Aggregator ID 2	Date Created	Aggregator ID 3	Date Created
AGG	109.56.87.123	109.57.8.23	N/A	01/08/2010 09:42:14	Pj42w6E3oXRfbVQcUzdJH2fZYus+t+	01/07/2010 13:15:28	N/A	N/A	N/A	N/A
AGG	217.198.32.175	N/A	255.255.225.242	01/08/2010 09:45:01	Pj42w6E3oXRfbVQcUzdJH2fZYus+t+	01/07/2010 13:15:28	N/A	N/A	N/A	N/A

Table 16-9 lists the information included in a RiskFort Trusted Aggregator Report:

Table 16-9. Trusted Aggregator Report Fields

Field	Description
Aggregator Name	The name of the aggregator.
Start IP Address	The IP address of the trusted aggregator.
End IP Address	The last address, if IP address range is specified.
Mask	The subnet mask value of the trusted aggregator IP address.
Date Added	The date when the second aggregator device ID was created.
Aggregator ID 1	The unique device ID of the trusted aggregator.
Date Created	The date when the first aggregator device ID was created.
Aggregator ID 2	The second device ID generated for the aggregator.
Aggregator ID 3	The third device ID generated for the aggregator.
Date Created	The date when the third aggregator device ID was created.

Negative IP Address Report

This report displays all negative IP addresses and ranges configured in the system. This report is available for both Proposed as well as Active data. (See [“Configuring Negative IP Addresses” on page 7-93](#) for more information on Negative IP List.)

To generate this report, specify the following options:

- The required **Organization Name**.
- The required **Ruleset Name**.

- The **Status**, which can be **ACTIVE** or **PROPOSED**.

Figure 16-9 displays the Negative IP Address Report page.

Figure 16-9 Negative IP Address Report

Negative IP Address Report				
<i>This report displays the details for the Negative IP address ranges that matched the criteria that you specified.</i>				
Export New Report				
Start IP Address	End IP Address	Mask	Information Source	Date Added
66.178.80.48	66.178.80.55	N/A	QUOVA	01/08/2010 09:56:34
85.236.136.15	85.236.236.79	N/A	QUOVA	01/08/2010 09:57:39
195.112.196.56	195.112.196.59	N/A	ARCOT	01/08/2010 09:58:23
198.165.197.192	198.165.197.223	N/A	ANONYMOUS PROXY	01/08/2010 09:59:01

Table 16-10 lists the information included in the Negative IP Address Report.

Table 16-10. Negative IP Report Fields

Fields	Description
Start IP Address	The IP address of the malicious user.
End IP Address	The last address, if IP address range specified.
Mask	The subnet mask value of the malicious user IP address.
Information Source	The vendor who supplied the negative IP range.
Date Added	The date when the entry was created.

Negative Country Report

This report displays the list of all negative countries configured in the system. This report is available for both Proposed and Active data. (See [“Configuring Negative Country List” on page 7-100](#) for more information on Negative Country List.)

To generate this report, specify the following options:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Status**, which can be **ACTIVE** or **PROPOSED**.

Figure 16-10 displays the Negative Country Report page.

Figure 16-10 Negative Country Report

Negative Country Report		
<i>This report displays the details for the Negative countries that matched the criteria that you specified.</i>		
		Export New Report
ISO Country Code	Country	Date Added
AF	AFGHANISTAN	01/08/2010 10:07:24
BD	BANGLADESH	01/08/2010 10:07:24
CN	CHINA	01/08/2010 10:07:24
IR	IRAN	01/08/2010 10:07:24
IQ	IRAQ	01/08/2010 10:07:24
KE	KENYA	01/08/2010 10:07:24
LY	LIBYA	01/08/2010 10:07:24
PK	PAKISTAN	01/08/2010 10:07:24

Table 16-11 explains the information that you see in the Negative IP List Report.

Table 16-11. Negative Country Report Fields

Fields	Description
ISO Country Code	The code assigned to every country by ISO.
Country	The name of the country.
Date Added	Date when the country was added to the list.

Exception User Report

This report displays the list of all Exception users configured in the RiskFort system.

To generate this report, you must specify:

- The **Date Range**.
- The required **Organization Name**.
- The **User Name**.

Figure 16-11 displays the RiskFort Exception User Report page.

Figure 16-11 Exception User Report

Exception User Report
This report displays the details for the Exception users that matched the criteria that you specified.

Export

New Report

Date Range:

From: 01/01/2010
 To: 01/08/2010

Start Date	End Date	User	Reason	Organization
01/07/2010 15:58:09	01/09/2010 15:58:09	EXUSER1	testing	DEFAULTORG
12/29/2009 15:58:09	01/07/2010 15:58:09	EXUSER2	testing	DEFAULTORG
01/03/2010 15:58:09	01/13/2010 15:58:09	EXUSER4	testing	DEFAULTORG
01/08/2010 15:58:09	01/10/2010 15:58:09	EXUSER5	testing	DEFAULTORG

Table 16-12 lists the information included in a RiskFort Exception Users Report:

Table 16-12. RiskFort Exception Users Report Fields

Fields	Description
Start Date	The date and time from which the user is considered an exception user in the system.
End Date	The date and time when the user stops being an exception user in the system.
User	The unique user name.
Reason	The reason for making the user an Exception User in the system.
Organization	The organization to which the administrator belongs.

Add-On Rules Report

The Add-On Rules Report provides an overall summary of all the Add-On rules that have been deployed for the specified organization. (See [“Working with Add-On Rules”](#) on page 12-185 for detailed information on Add-On rules.)

To generate this report, you must specify:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Status** of the target information.

Figure 16-12 displays an Add-On Rules Report page.

Figure 16-12 Add-On Rules Report

Add-On Rules Report						
<i>This report displays the overall summary of the deployed Add-On rules that matched the criteria that you specified.</i>						
					Export	New Report
Rule Name	Enabled	Rule Mnemonic	Library Name	Rule Type	Parameters	Description
High Amount Check	NO	HIGHAMTCHK	rfrulenicnumericcomparison_ex	AMOUNT_CHECK	THRESHOLD=500:840]	This rule checks for transaction amounts that exceed \$500.
High Device Velocity from Unexpected Locations	NO	HIGHDEVICEVELOCITYCHECK	rfrulecombination	COMBINATION_RULE	EXP= DEVICEVELOCITY AND NOT (COUNTRY IN \$\$SAFE_COUNTRIES)	This rule checks for transactions with high Device Velocity from unexpected locations.

Table 16-13 lists the information included in an Add-On Rules Report:

Table 16-13. Add-On Rules Report Fields

Fields	Description
Rule Name	The name of the Add-On rule.
Enabled	The indication whether the rule is being used or not at the time the report is run.
Rule Mnemonic	The short name of the Add-On rule.
Library Name	The name of the <code>.dll</code> or <code>.so</code> file associated with the rule.
Rule Type	The Add-On rule type created by the Master Administrator.
Parameters	The default value(s) that the rule must check for each transaction in real time.
Description	The detailed description of what the rule does for later reference.

Rules Data Report

The Rules Data Report displays the summarized data for the selected Simple List that has been uploaded for an organization. (See [“Working with Add-On Rules” on page 12-185](#) for detailed information on List data and how to upload a list to be used by an Add-On rule.)

To generate this report, you must specify:

- The required **Organization Name**.

- The required **Ruleset Name**.
- The **Status** of the target information.
- The uploaded **Dataset Name** (or the name of the list.)

Figure 16-13 displays the Rules Data Report page (for an uploaded list called `SAFE_COUNTRYIES`.)

Figure 16-13 Rules Data Report

Rules Data Report	
<i>This report provides the list data.</i>	
Export New Report	
Data	Date Added
India	03/22/2010 12:10:05
US	03/22/2010 12:10:05
Denmark	03/22/2010 12:10:05
Iceland	03/22/2010 12:10:05
Norway	03/22/2010 12:10:05
Sweden	03/22/2010 12:10:05
Canada	03/22/2010 12:10:05
Germany	03/22/2010 12:10:05
Italy	03/22/2010 12:10:05

Table 16-14 lists the information included in an Rules Data Report:

Table 16-14. Rules Data Report Fields

Fields	Description
Data	The corresponding entries (or data values) in the list.
Date Added	The date when the corresponding entry was added.

Rules Data Classification Report

The Rules Data Classification Report displays the summarized data for the selected Mapping List that has been uploaded for an organization. (See [“Working with Add-On Rules” on page 12-185](#) for detailed information on List data and how to upload a list to be used by an Add-On rule.)

To generate this report, you must specify:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Status** of the target information.

- The uploaded **Dataset Name** (or the name of the list.)

Figure 16-14 displays the Rules Data Classification Report page (for an uploaded list called `MERCHANT_CATEGORY_MAPPING`.)

Figure 16-14 Rules Data Classification Report

Rules Data Classification Report

This report provides data classification.

[Export](#)
[New Report](#)

«« 1 2 3 »»

Param Value	Category	Date Added
800florals	Flower Delivery	03/23/2010 06:16:40
AdultReviews	Porn	03/23/2010 06:16:41
Amazon	Online Shopping	03/23/2010 06:16:41
American Airlines	Airline	03/23/2010 06:16:41
BEST-BUY-DEAL	Online Shopping	03/23/2010 06:16:41
British Airways	Airline	03/23/2010 06:16:41
Casinogamblingweb	Gambling	03/23/2010 06:16:41
Cilphunter	Porn	03/23/2010 06:16:41
Costco	Online Shopping	03/23/2010 06:16:41
eBay	Online Shopping	03/23/2010 06:16:41

«« 1 2 3 »»

Table 16-15 lists the information included in an Rules Data Classification Report:

Table 16-15. Rules Data Classification Report Fields

Fields	Description
Parameter Value	The corresponding entry (or data value) in the list.
Category	The corresponding category (defined by an administrator) to which the entry belongs.
Date Added	The date when the entry was added.

Case Management Reports

The Fraud Statistics Report is the only Case Management-related report available in the system. See section “[Generating the Fraud Statistics Report](#)” on page 15-265 in Chapter 15, “[Managing Cases](#)” for detailed information on this report.

Generating Reports

This section covers:

- [Notes for Generating Reports](#)
- [Generating Reports](#)

Notes for Generating Reports

While generating reports, remember that:

- The administrator can *only* generate the reports of the organizations on which they have the scope.
- The administrator can generate the report of their subordinate or peers.

For example, an Organization Administrator (OA) can generate the reports of an OA and User Administrator (UA).

- If the administrator role is derived by using a custom role, then the derived administrator role belongs to the same level as that of the parent.

For example, if you derive an administrator *MyGlobalAdmin* from GA, then *MyGlobalAdmin* is considered to be a GA even though you might have assigned *MyGlobalAdmin* less number of privileges compared to an OA or UA.

- If you are using Oracle database, then ensure that you have enabled the [UNLIMITED TABLESPACE](#) privilege.

Generating Reports

To generate any of the administrator- or RiskFort-specific reports:

1. Ensure that you are logged in with proper credentials (MA, GA, OA, or UA.)
2. Activate the **Reports** tab in the main menu.
3. If you want to generate:
 - Administrator activity report, then click the **Administrator Reports** sub-menu.
 - RiskFort-specific report, then click the **RiskFort Reports** sub-menu.

The corresponding links for the report type appear in the left-handle task panel.

4. Based on the report you want to generate, click the required link from the left-hand sub-menu.

5. Specify one or more of the following criteria, as applicable, to view the report:
 - The **Date Range** from the drop-down list.
 - or
 - A pre-defined date range in the **From** and **To** fields.
6. Depending on the report, additionally you might have to specify the following:
 - **Organization Name** for the required organizations whose data you want to include in the report.
 - **User Name** (or **Administrator Name**), based on the report you want to generate:
 - Enter a user name (for User Activity reports.)
 - or
 - Enter the administrator name (for Administrator Activity reports.)
 - **Ruleset Name** for the required ruleset whose data you want to include in the report.
7. Click **Display Report** to generate the report based on the criteria you specified.

Exporting Reports

The Administration Console provides the ability to export reports to a file. By exporting a report, you can save a local copy of the report, which enables you to track trends. You can also work with the saved report data in another application.

The exported reports are generated in the comma-separated value (CSV) format that can be viewed by using text editors and spreadsheet applications, such as Microsoft Excel. The export option is available through the **Export** button, which appears at the top-right of every rendered report.

To export a report to a local file:

1. Generate the required report. See section, [“Generating Reports”](#) for detailed instructions to do so. The report opens.
2. Click **Export**.
You are prompted to save or open the report.
3. Click **Open (with)** or **Save (file)**. If you choose to save the report, then you must specify the download location.

This file can later be viewed by using the appropriate application.

Chapter 17

Tools for System Administrators

This chapter discusses the tools provided by RiskFort that administrators can use to monitor and manage the system. These tools are available in the following location:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

On UNIX Platforms:

```
<install_location>/arcot/bin/
```

This chapter describes the following tools:

- [DBUtil: RiskFort Database Tool](#)
- [arrfversion: RiskFort Modules Version Display Tool](#)
- [arrfadmin: Server Refresh and Shutdown Tool](#)
- [arrfserver: RiskFort Server Tool](#)
- [arrfupload: Quova Data Upload Tool](#)

DBUtil: RiskFort Database Tool

During RiskFort installation, the installer collects the information to connect to the RiskFort database. After the installation is completed, the information for the RiskFort Server to connect to the database is stored in the encrypted format in a file called `securestore.enc`. This file stores the following encrypted information that you need to connect to the RiskFort database:

- Master key name
- Database user name and password

If for some reason you need to change the master key value or add a new database user name, password, or DSN after installation, then you can use [DBUtil](#) to:

- [Set up the Master Key](#)

- [Insert a Database User Name and Password](#)
- [Use Additional DBUtil Options](#)

Set up the Master Key

Specified during the installation, the *master key* is used to encrypt the values in the `securestore.enc` file. It also encrypts all encryption keys that are stored in the RiskFort database.

If for some reason you need to change the master key value in `securestore.enc`, then:



Important: The following procedure *must* be done only if the master key setup failed during the installation. Contact Arcot Technical Support at support@arcot.com for help.

1. Backup the current `securestore.enc` file.
The current `securestore.enc` is available at:
 - **On Windows**
`<install_location>\Arcot Systems\conf\`
 - **On UNIX-based Platforms**
`<install_location>/arcot/conf/`
2. Ensure that you delete the current `securestore.enc`.
3. Navigate to the location where the tool is available:

- **On Windows**
`<install_location>\Arcot Systems\bin\`
- **On UNIX-based Platforms**
`<install_location>/arcot/bin/`

4. Run the following command:

dbutil -init encryptKeyName

The tool re-creates `securestore.enc` with the master key name that you specify.

Insert a Database User Name and Password

The RiskFort installer automatically configures the database `username/password` and database `DSN/password` information in `securestore.enc`. However, if you need to insert this information manually, the you must use the `dbutil -insert` option to do so. This option adds the required values to the file instead of overwriting or updating them.



Note: The `DSN` and `password` information is used by RiskFort and database servers, while `username` and password information is used by Java components.

1. Navigate to the location where the `DBUtil` tool is available:
2. To insert the supplied database `username` and `password` values in `securestore.enc`, enter the following command:

```
dbutil -pi dbUser dbPassword
```

In the preceding command, `dbUser` is the database user name and `dbPassword` is the password associated with the specified user name. For example:

```
dbutil -pi arcotuser dbpassword
```

Use Additional DBUtil Options

Table 17-1 lists the options for `dbutil`. In this table, *key-value* pair refers to either DSN, password, or database username/password pair. The DSN/password is used by RiskFort Server, while user name/password is used by Administration Console and User Data Service.

Table 17-1. Additional DBUtil Options

Option	Description
<code>-h</code>	Displays the Help for the tool. Syntax: <code>dbutil -h</code>
<code>-init</code>	Creates a new <code>securestore.enc</code> , if it was not found in the <code>conf</code> directory. Syntax: <code>dbutil -init key</code> For example: <code>dbutil -init MasterKeyNew</code> <code>dbutil -init RiskFortDatabaseMKNew</code> Important: This command succeeds only if there is no <code>securestore.enc</code> in the <code>conf</code> directory.
<code>-pd</code>	Deletes the specified key-value pair from <code>securestore.enc</code> . Syntax: <code>dbutil -pd key</code> For example: <code>dbutil -pd RiskFortDatabaseDSNold</code> <code>dbutil -pd Jack</code>

Table 17-1. Additional DBUtil Options

Option	Description
-pi	Inserts an additional key-value pair into <code>securestore.enc</code> (as discussed in the previous section, “Insert a Database User Name and Password”). Syntax: <pre>dbutil -pi key value</pre> For example: <pre>dbutil -pi RiskFortBackupDSN dbapassword dbutil -pi Jack userpassword</pre> Important: Each key can only have one value. If you have already inserted a key-value pair, then you cannot insert another value for the same key.
-pu	Updates the value for an existing key-value pair in <code>securestore.enc</code>. This feature can be used when you need to update the database password. Syntax: <pre>dbutil -pu key value</pre> For example: <pre>dbutil -pu RiskFortDatabaseDSN newPassword dbutil -pu Jack userPassword</pre>

arrfversion: RiskFort Modules Version Display Tool

The `arrfversion` tool enables you to check and display the versions of the *RiskFort Rule and Plugin modules* (`.dll` files on Windows and `.so` on UNIX-based platforms) that are available in the following directories (relative to `ARCOT_HOME`):

- `/bin/`
- `/plugin/rules/`
- `/plugin/rules/addon/`

In case of deployment- and operation-related problems, when you contact Arcot Technical Support (support@arcot.com), it is a great practice if you specify the version of the deployed modules. This helps in faster identification and resolution of a problem.

Syntax:

The syntax to use the tool is:

```
arrfversion <library1_path> [<library2_path> ...]
```

In the preceding syntax, the `<libraryN_path>` string specifies the name of an individual module, such as:

- `aradminprotocol.dll` on Windows
- `libaradminprotocol.so` on UNIX-based platforms

If you do not specify the absolute path of the library module, then the specified module is looked up in the folders specified by the standard environment variables. For example:

- `%PATH%` for Windows
- `$LD_LIBRARY_PATH` for UNIX-based platforms

Examples:

Windows:

```
arrfversion ScoreEngine.dll
```

UNIX-based Platforms:

```
arrfversion /opt/arcot/plugins/rules/libaradminprotocol.so
```

arrfadmin: Server Refresh and Shutdown Tool

Many configuration changes that you make might need the server to be refreshed. For example, all `.ini` file changes need the server to be restarted. Also, some changes that you make by using Administration Console also require the server either to be restarted or refreshed. In such cases, the Administration Console informs you to refresh or restart, as applicable.



Note: The refresh option ensures that the server does not take any down time. Very few configuration changes need the server to be restarted.

The `arrfadmin` tool enables you to gracefully shut down the server or refresh its cache without restarting it. In case of graceful shutdowns, the server allows all existing requests to complete while not accepting any new requests.

Before You Use the Tool

Before you can use the tool, you must configure the settings in `riskfortadminclient.ini`. This file is available at the following location:

On Windows:

```
<install_location>\Arcot Systems\conf\
```

On UNIX Platforms:

```
<install_location>/arcot/conf/
```



Note: See Appendix B, "Configuration Files and Options", in the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for detailed information related to `riskfortadminclient.ini`.

The minimal parameters in this file that must be configured for the tool to work properly are listed in [Table 17-2](#).

Table 17-2. Minimum Parameters to Set in riskfortadminclient.ini

Parameter	Default	Description
Host	localhost	The host name or the IP Address of the system where RiskFort Server is running.
Port	7980	The port number on which server is listening to server management requests.
Transport	tcp	The transport mode for server management listener. The possible values are: • TCP • SSL

These settings ensure the typical TCP-based communication between the tool and the RiskFort Server. If you want to configure two-way SSL communication between the two, refer to the section, [“Configuring the Tool for Two-Way SSL Communication with the Server”](#).

Using the Tool

Syntax:

After you configure the minimal settings in `riskfortadminclient.ini`, you can use the tool. You can use the tool by using one of the following syntaxes:

- **arrfadmin** [*<options>*]

If you use the preceding syntax, then you must ensure that you have configured the parameters in `riskfortadminclient.ini` (listed in [Table 17-2](#).)

- **arrfadmin** *<server_ipaddress>* *<server_adminport>* [*<options>*]

[Table 17-3](#) lists the parameters used by the `arrfadmin` tool.

Table 17-3. arrfadmin Server Connectivity Parameters

Parameters	Description
Host or server_ipaddress	The IP address or the host name at which the RiskFort Server or the Case Management Queuing Server is available.
Port or server_adminport	The port number at which the RiskFort Server or the Case Management Queuing Server listens to the operations requests. Note: By default, the RiskFort Server is available on port 7980 .

[Table 17-4](#) lists the *<options>* supported by the tool.

Table 17-4. arrfadmin Options

Options	Description
-h	This option displays the Help for the tool. It does not need any parameters. For example: <pre>arrfadmin -h</pre>
-d	This option is used to initiate the graceful shutdown of the server. For example: <pre>arrfadmin -d</pre> or <pre>arrfadmin 10.150.1.40 7980 -d</pre>
-r	This option is used to send a refresh request to the server. For example: <pre>arrfadmin -r</pre>

Configuring the Tool for Two-Way SSL Communication with the Server

To configure the `arrrfadmin` tool for two-way SSL communication with the RiskFort Server, you must:

1. [Step 1: Edit riskfortadminclient.ini](#)
2. [Configure the Server Management Protocol](#)

Step 1: Edit riskfortadminclient.ini

To edit this file:

1. Navigate to the `conf` directory in the `ARCOT_HOME`, where the `riskfortadminclient.ini` file is available.
2. Ensure that the values for `Host` and `Port` parameters in the file point to the required RiskFort Server instance.
3. Specify the required values for the parameters listed in [Table 17-5](#).

Table 17-5. Two-Way SSL Parameters to Set in riskfortadminclient.ini

Parameter	Default	Description
Transport	<code>tcp</code>	Specify SSL as the transport mode.
SSLClientKey	No Default	Specify the absolute path of the base64-encoded (PEM formatted) SSL key to be used by the <code>arrrfadmin</code> tool.
SSLClientCertChain	No Default	Specify the absolute path of the base64-encoded (PEM formatted) SSL certificate or certificate chain to be used by the <code>arrrfadmin</code> tool.
SSLServerCACert	No Default	Specify the absolute path of the base64-encoded (PEM formatted) SSL CA certificate that the <code>arrrfadmin</code> tool must trust during the SSL communication between the tool and the RiskFort Server. For example: <code>ServerCACert=<install_location>/Arcot Systems/certs/riskfort_ca.pem</code>



Important: The key associated with the certificate must be unencrypted. If the private key is in PEM format and encrypted, then the Administration Console will display an error message.

Configure the Server Management Protocol

To configure RiskFort Server Management protocol for two-way SSL:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **System Configurations** section, click the **Protocol Management** link to display the Protocol Configuration page.
5. Perform the following steps to configure the RiskFort Server Management protocol for SSL:
 - a. In the **Enabled** column, ensure that the check box corresponding to **Server Management** is selected.
 - b. In the **Port** column, specify port number if you want to configure the Server Management protocol at a port number different than the default.
 - c. In the **Transport Security** column, select **SSL** from the drop-down list.
 - d. In the **Client Store** column, select the required trust store that contains the root certificate of the trusted Certificate Authority (CA).



Note: If there is no trust store available to be selected, then the Master Administrator must first configure it by using the **Trusted Certificate Authorities** link under the **System Configuration** section.

- e. In the **SSL Certificate Details** column:
 - i. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the SSL certificate chain for the server.



Note: The certificates in the chain *must* start from Leaf certificate, Intermediate CA certificates, and then Root certificate.

- ii. Click **Browse** against **Private Key** to navigate to the appropriate location and upload the corresponding private key of the certificate.



Note: The certificate chain and the private key, both *must* be in PEM format private key uploaded must be not be password protected.

- f. Click **Save** to save the changes.
6. Click **Save** after you complete the configurations on the page.
7. Refresh the RiskFort Server instance for which you made the preceding changes. See [“Restarting a Server Instance” on page 4-54](#) for instructions on how to do this.

arrfserver: RiskFort Server Tool

The `arrfserver` tool is the core risk evaluation server module that can also be run from the command line in interactive mode to enable you to configure:

- The authentication and authorization settings for RiskFort Web services.
- The RiskFort settings that are either used rarely or are needed only under certain deployment scenarios.
- The RiskFort configurations that are not exposed through the Administration Console.

Running the Tool in Interactive Mode

The tool provides the `-i` option to run it in the interactive mode. In this mode all the server configurations are done in a similar fashion as that in the service mode, except that the listeners are not started.

When run in this mode, the server starts its own console prompt (`#`). To run the `arrfserver` tool:

1. Navigate to the location where the tool is available:
 - **On Windows:**

```
<install_location>\Arcot Systems\bin\
```
 - **On UNIX-based platforms:**

```
<install_location>/arcot/bin/
```

2. Run the following command:

- **On Windows:**

```
arrfserver -i
```

- **On Unix-based platforms:**

```
riskfortserver -i
```

The tool starts in interactive mode.

3. Specify the options listed in [Table 17-6](#) to perform the required task.

Table 17-6. arrfserver Options

Option	Description
?	Lists the commands for the <i>all</i> options supported by <code>arrfserver</code> . For example, if you enter <code>help setsaconf</code> , then the usage of the command is briefly explained.
??	Searches the commands based on the pattern you provide. For example, if you enter <code>?? conf</code> , then all the tool options that match the pattern are displayed.
<code>setsaconf</code>	Enables you to configure the Web Services APIs that are provided by RiskFort Server for authentication and authorization. Enter <code>1</code> for securing the access or <code>0</code> for regular access.
<code>q</code>	Closes the interactive mode.

arrfupload: Quova Data Upload Tool

RiskFort uses Quova data to identify the geo-location information of a user by using the IP address of the system from which the transaction originated. It then uses this data to evaluate Negative Country, Negative IP, and Zone Hopping rules.

See “Configuring Negative IP Types” on page 7-96, “Configuring Negative IP Addresses” on page 7-93, and “Configuring Zone Hopping” on page 7-109 for more information.

To know more about Quova and their services, go to:

<http://www.quova.com>



Note: You must download the Quova data regularly. Data files for GeoLocation-related information must be downloaded every week, while the Anonymizer-related data files must be downloaded every month. Contact Arcot Support at support@arcot.com for the details about the download procedure.

The *Arcot RiskFort Data Upload Tool* ([arrfupload](#)) is a command-line utility that enables you to upload the geolocation data from Quova files to the RiskFort database.

Before You Use the Tool

The [riskfortdataupload.ini](#) file controls the behavior of the Arcot RiskFort Data Upload tool. It is available at the following location:

On Windows:

```
<install_location>\Arcot Systems\conf\
```

On UNIX Platforms:

```
<install_location>/arcot/conf/
```

You must configure the parameters in this file ([Table 17-7](#)) before you can use the tool.

Table 17-7. Configuration Parameters for riskfortdataupload.ini

Parameter	Default	Description
Tables	Do Not Load	The tables that the user can work with. Possible values are: • GeoPoint • Anonymizer
Load	0	The indicator whether to upload the data to the table or not. Possible values are: • 0 (Do not load) • 1 (Load)

Table 17-7. Configuration Parameters for riskfortdataupload.ini

Parameter	Default	Description
Swap	0	The indicator whether to switch RiskFort configuration to start using the table where GeoPoint or GeoAnonymizer data has just been uploaded. Important: The RiskFort Server cache must be refreshed (by using the <code>arrfadmin -r</code> command) after this change. Possible values are: • 0 (Do not swap) • 1 (Swap)
Filename	--	The name of the file from which the Quova data has to be loaded. Important: You must mention the absolute path to the file, along with the file name.



Note: If both, `Load` and `Swap` are set to 1, then first the table is loaded and then is swapped.

Using the Tool

This tool is available at the following location:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

On UNIX Platforms:

```
<install_location>/arcot/bin/
```

This tool uses the database information in the `arcotcommon.ini` file to connect to the RiskFort database and uses the `username` and `password` specified in the `securestore.enc` file to authenticate to the database.

Syntax:

Run the following command to use the tool:

arrfupload <option>

Important: The Quova information that you upload by using this tool is not available until you refresh the RiskFort Server cache by using the `arrfadmin -r` command.

Table 17-8 lists the options supported by the utility.

Table 17-8. arrfupload Options

Options	Description
-help	Lists <i>all</i> options supported by the tool, followed by the brief usage of the option.
-config	This option is used to read information from <code>riskfortdataupload.ini</code> (the configuration file used by the tool) and perform the required action. This option uses the following flags: • Tables: The set of tables the user wants to update. The values allowed are either <code>Geopoint</code> or <code>Anonymizer</code>. If neither is specified, then no data is uploaded. This option does not have any default value. • Load: If set to <code>1</code>, indicates that the data will be uploaded and if set to <code>0</code> indicates that data will not be uploaded. The default is value is <code>0</code>. Important: If set to <code>1</code>, the <code>Filename</code> and <code>Tables</code> flags <i>must</i> be set. • Swap: If set to <code>1</code>, indicates that the table will be swapped and if set to <code>0</code> indicates that table will not be swapped. The default is value is <code>0</code>. Important: This flag is valid only if the <code>Tables</code> flag is set correctly. Also, you must refresh the RiskFort Server cache to be able to use the new table. • Filename: Indicates the name and the path of the Quova file that contains the data to be uploaded. Important: This flag is valid only if the <code>Load</code> flag is set to <code>1</code>.

Table 17-8. arrfupload Options

Options	Description
-tnames	This option is used to display the current ARQGeoPoint and ARQGeoAnonymizer tables being used by the RiskFort database.
-prompt	This option is used to display an interactive command-line menu that enables the user to select the table (ARQGeoPoint or ARQAnonymizer) they want to update using the latest Quova data. Based on the table specified by the user, a sub-menu with following options appears: • Load Quova Data: Depending on the set of tables chosen from the main menu, enables the data to be loaded in to the specified table. You must specify the name of the file from which Quova data has to be loaded along with the path where this file is available. • Swap Quova Tables: Depending on the set of tables chosen from the main menu, enables the user to swap tables. • Exit to the previous menu: Enables the user to the main menu. • Exit the program: Enables the user to exit from the tool.

Appendix A

RiskFort Logging

To effectively manage the communication between RiskFort Server and your application, it is necessary to get information about the activity and performance of the Server and other components, as well as any problems that might have occurred.

This appendix describes the various log files supported by RiskFort, the severity levels that you will see in these files, and the formats of these log files. It covers the following topics:

- [About the Log Files](#)
- [Format of the RiskFort Server and Case Management Server Log Files](#)
- [Format of UDS and Administration Console Log Files](#)
- [Supported Severity Levels](#)

About the Log Files

The RiskFort log files can be categorized as:

- [Installation Log File](#)
- [Transaction Log Files](#)
- [UDS Log File](#)
- [Administration Console Log File](#)

All logging-related parameters (specified under the `[arcot/riskfort/logger]` section) are controlled by the `riskfortserver.ini` file. These logging configuration options include:

- **Specifying log file name and path:** RiskFort enables you to specify the directory for writing the log files and storing the backup log files. Specifying the diagnostic logging directory allows administrators to manage system and network resources.
- **Log file size:** The maximum number of bytes the log file can contain. When the log files reach this size, a new file with the specified name is created and the old file is moved to the backup directory.

- **Using log file archiving:** As RiskFort components run and generate diagnostic messages, the size of the log files increases. If you allow the log files to keep increasing in size, then the administrator must monitor and clean up the log files manually. RiskFort enables you to specify configuration options that limit how much log file data is collected and saved. RiskFort lets you specify the configuration option to control the size of diagnostic logging files. This lets you determine a maximum size for the log files. When the maximum size is reached, older log information is moved to the backup file before the newer log information is saved.
- **Setting logging levels:** RiskFort also allows you to configure logging levels. By configuring logging levels, the number of messages saved to diagnostic log files can be reduced. For example, you can set the logging level so that the system only reports and saves critical messages. See [“Supported Severity Levels” on page A-319](#) for more information on the supported log levels.
- **Specifying time zone information:** RiskFort enables you to either use the local time zone for time stamping the logged information or use GMT for the same.

Installation Log File

When you install RiskFort, the installer records all actions that it performs in the [Arcot_RiskFort_InstallLog.log](#) file. The information in this file is very useful in identifying the source of the problems if the RiskFort installation did not complete successfully.

The default location of this file is:

Windows:

```
<install_location>\Arcot Systems\logs\
```

UNIX-Based:

```
<install_location>/arcot/logs/
```

Transaction Log Files

The transaction logs consist of:

- [RiskFort Server Log](#)
- [Case Management Server Log File](#)

RiskFort Server Log

RiskFort records all requests processed by the server and related actions in the `arcotriskfort.log` file. The default location of this file is:

Windows:

```
<install_location>\Arcot Systems\logs\
```

UNIX-Based:

```
<install_location>/arcot/logs/
```



Note: You cannot use the RiskFort logger to configure your application's logs. You can access these logs by using the tool used by the third-party application server (such as Apache Tomcat or IBM Websphere) that is hosting your application.

All logging-related parameters (specified under the `[arcot/riskfort/logger]` section) are controlled by the `riskfortserver.ini` file, which is available in the `conf` folder in `ARCOT_HOME`.

Case Management Server Log File

When you deploy the Case Management Server module and subsequently start it, the details of all its actions and processed requests are recorded in the `arcotriskfortcasemgmtserver.log` file. The default location of this file is:

Windows:

```
<install_location>\Arcot Systems\logs\
```

UNIX-Based:

```
<install_location>/arcot/logs/
```



Note: You cannot use the RiskFort logger to configure your application's logs. You can access these logs by using the tool used by the third-party application server (such as Apache Tomcat or IBM Websphere) that is hosting your application.

All logging-related parameters (specified under the `[arcot/riskfortcasemgmtserver/logger]` section) are controlled by the `riskfortcasemgmtserver.ini` file, which is available in the `conf` folder in `ARCOT_HOME`.

UDS Log File

All User Data Service (UDS) information and actions are recorded in the `arcotuds.log` file. This information includes:

- UDS database connectivity information
- UDS database configuration information
- UDS instance information and the actions performed by this instance

The information in this file is very useful in identifying the source of the problems if the Administration Console could not connect to the UDS instance. The default location of this file is:

Windows:

```
<install_location>\Arcot Systems\logs\
```

UNIX-Based:

```
<install_location>/arcot/logs/
```

The parameters that control logging in this files can be configured by using the `udsserver.ini` file, which is available in the `conf` folder in `ARCOT_HOME`.

In addition to the logging level, log file name and path, the maximum file size (in bytes), and archiving information, you can also control the layout of the logging pattern for UDS by specifying the appropriate values for

`log4j.appender.debuglog.layout.ConversionPattern`.

See section, “[Format of UDS and Administration Console Log Files](#)” on page A-318 for the details of the default format used in the file.

Administration Console Log File

When you deploy the Administration Console and subsequently start it, the details of all its actions and processed requests are recorded in the `arcotadmin.log` file. This information includes:

- Database connectivity information
- Database configuration information
- Instance information and the actions performed by this instance
- UDS configuration information
- Other Administration Console information specified by the Master Administrator, such as cache refresh

The information in this file is very useful in identifying the source of the problems if the Administration Console does not start up. The default location of this file is:

Windows:

```
<install_location>\Arcot Systems\logs\
```

UNIX-Based:

```
<install_location>/arcot/logs/
```

The parameters that control logging in this files can be configured by using the `adminserver.ini` file, which is available in the `conf` folder in `ARCOT_HOME`.

In addition to the logging level, log file name and path, the maximum log file size (in bytes), log file archiving information, you can also control the layout of the logging pattern for the console by specifying the appropriate values for

```
log4j.appender.debuglog.layout.ConversionPattern.
```

See section, “[Format of UDS and Administration Console Log Files](#)” on page A-318 for the details of the default format used in the file.

Format of the RiskFort Server and Case Management Server Log Files

[Table A-1](#) describes the format of the entries in the RiskFort logger, `arcotriskfort.log`, as discussed in the section, “[RiskFort Server Log](#)” on page A-315.

Table A-1. RiskFort Logging Format

Column	Description
Time Stamp	Time the entry was logged, translated to the specified time zone. The format of logging this information is: <code>www mmm dd HH:MM:SS.mis yy timezone</code> In the preceding format: <code>www</code> represents weekday. <code>mis</code> represents milliseconds. <code>timezone</code> represents the time zone you specified in the <code>riskfortserver.ini</code> file.
Log Level (or Severity)	The severity level of the logged entry. See “ Supported Severity Levels ” for detailed information.

Table A-1. RiskFort Logging Format

Column	Description
Process ID (pid)	The ID of the process that logged the entry.
Thread ID (tid)	The ID of the thread that logged the entry.
Transaction ID	The ID of the transaction that logged the entry.
Module ID (Deprecated)	The ID of the RiskFort module (such as Rules Engine or Scoring Engine) that logged the entry. Note: This is a deprecated entry and always shows 0.
Message	The message logged by the Server in the free-flowing format. Note: The granularity of this message depends on the Log Level that you set in riskfortserver.ini .

Format of UDS and Administration Console Log Files

[Table A-2](#) describes the format of the entries in the following loggers:

- [arcotuds.log](#) ([UDS Log File](#))
- [arcotadmin.log](#) ([Administration Console Log File](#))

Table A-2. UDS and Administration Console Logging Format

Column	Associated Pattern (In the Log File)	Description
Time Stamp	%d{yyyy-MM-dd hh:mm:ss,SSS z} :	The time when the entry was logged. This entry uses the application server time zone. The format of logging this information is: yyyy-MM-dd hh:mm:ss,SSS z Here: • SSS represents milliseconds. • z represents the time zone.
Thread ID	[%t] :	The ID of the thread that logged the entry.
Log Level (or Severity)	%-5p :	The severity level of the logged entry. See “Supported Severity Levels” for more information.

Table A-2. UDS and Administration Console Logging Format

Column	Associated Pattern (In the Log File)	Description
Logger Class	%-5c{3} (%L) :	The name of the logger that made the log request.
Message	%m%n :	The message logged by the Server in the log file in the free-flowing format. Note: The granularity of the message depends on the Log Level that you set in the log file.

Refer to the following URL for customizing the [PatternLayout](#) parameter in the UDS and Administration Console log files:

<http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html>

Supported Severity Levels

A *log level* (or *severity level*) enables you to specify the level of detail of the information stored in the RiskFort logs. This also enables you to control the rate at which the log file will grow.

[Table A-3](#) describes the log levels that you see in all log files, in the *decreasing* order of severity.

Table A-3. RiskFort Log Levels (in Decreasing Order of Severity)

Log Level		Description
0	FATAL	Use this log level for serious, non-recoverable errors that can cause the abrupt termination of the RiskFort service.
1	WARNING	Use this log level for undesirable run-time exceptions, potentially harmful situations, and recoverable problems that are not yet FATAL .
2	INFO	Use this log level for capturing information on run-time events. In other words, this information highlights the progress of the application, which might include changes in: • Server state, such as start, stop, and restart. • Server properties. • State of services. • State of a processes on the Server.
3	LOW DETAIL	Use this log level for logging detailed information for debugging purposes. This might include process tracing and changes in Server states.



Note: When you specify a log level, messages from all other levels of *higher* significance are reported as well. For example if the `LogLevel` is specified as `3`, then messages with log levels of `FATAL`, `WARNING`, and `INFO` level are also captured.

Sample Entries for Each Log Level

The following subsections show a few sample entries (based on the Log Level) in the **RiskFort** log file.

FATAL

```
May 27 18:31:01.585 2010 GMT FATAL: pid 4756 tid 5152: 0: 0: Cannot
continue due to ARRF_LIB_init failure, SHUTTING DOWN
```

WARNING

```
May 24 14:47:39.756 2010 GMT WARNING: pid 5232 tid 5576: 0: 110000:
EVALHTTPCALLOUT : Transport Exception : create: No Transports Available
```

INFO

```
May 24 14:41:43.758 2010 GMT INFO: pid 3492 tid 4904: 0: 109002: Error
in ArPFExtRuleSetEval::evaluate Could not get user context (two
parallel requests)
```

```
May 25 10:01:28.131 2010 GMT WARNING: pid 1048 tid 3104: 8: 0: Error in
ArRFCasestatus::startInit: No data found
```

DETAIL

```

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering USERRISKEVALVELOCITY Rule Evaluation
function

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE: VELOCITY_DURATION=[60],
VELOCITY_DURATION_UNIT=[MINUTES],                VELOCITY_TRANSACTION_COUNT=[5]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering UserRiskEvalVelocityRule
durationToTimeConvertor

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting UserRiskEvalVelocityRule
durationToTimeConvertor

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering UserRiskEvalVelocityRule
callUserEvalVelocityRule

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering
ArUserRiskEvalVelocityDBO::decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT INFO: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting
ArUserRiskEvalVelocityDBO::decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting UserRiskEvalVelocityRule
callUserEvalVelocityRule

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.RESULT=[0]

```

```
May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:  
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.DETAIL=[RESULT=0;TCOUNT=2;  
ACT=mecction]
```

```
May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:  
USERRISKEVALVELOCITYRULE : Exiting USERRISKEVALVELOCITY Rule Evaluation  
function
```


Appendix B

Glossary

Aggregator	Third-party vendors who provides account aggregation services by collating user information across multiple enterprises.
Add-On Rule	Additional Risk Evaluation rule that ships with RiskFort.
Authentication	A process by which an entity proves that it is who it claims to be.
Callout	Custom program executing externally (outside RiskFort).
Certificate	See Digital Certificate .
Credential	A proof of user identity. Digital credentials may be stored on hardware such as smart-cards or USB tokens or on the server. They are verified during authentication.
Customer Support Representatives (CSR)	Administrators responsible for the day-to-day operations related to users of the security system. For example, Administrators can assist users with enrollment, resetting users passwords, and generating enrollment reports.
Device Velocity	Number of transactions from the same device within a specified time.
Digital Certificate	A digital document that vouches for the identity and key ownership of an individual, a computer system, or an organization. This authentication method is based on the public-key cryptography (PKI) method.
Encryption	The process of scrambling information in a way that disguises its meaning.
Exception User	User “known” to RiskFort and is excluded from risk assessments for a specified period of time.
Evaluation Callout	Callout that runs after all Evaluation Rules and contains custom risk evaluation logic.
Evaluation Rule	Pre-configured RiskFort logic that is applied to the incoming transaction data.
Extensible Element	Additional element pertaining to a transaction that is used by Add-On Rules for risk evaluation.
Global Administrator	An administrator responsible for setting up Customer Support Representatives (CSR) accounts and configuring the system.

Increased Authentication	The Risk Advice given by RiskFort, if the current transaction is considered unsafe by RiskFort. For example, if a user does a transaction of high amount for the first time. Under such circumstances, the user is asked to re-authenticate to the authentication server through stronger authentication method.
Master Administrator	The highest level of RiskFort administrator, whose primary responsibilities are to initialize RiskFort and create Global Administrator accounts.
Negative IP Address	IP address that has been the origin of known anonymizer proxies or fraudulent or malicious transactions in the past.
Negative Country	Country from which fraudulent or malicious transactions are known to have originated in the past.
Non-Terminating Rule	The rule alone does not determine overall Risk Score . It requires other rules for the purpose.
One-Way SSL	Client application verifies the identity of the server application (by accepting server's Digital Certificate) before the SSL session is established.
Private Key	One of a pair of keys used in PKI, which is kept secret and can be used to decrypt or encrypt data.
Public Key	One of a pair of keys used in PKI, which is distributed freely and is published as part of a certificate. It is typically used to encrypt data sent to the public key's owner, who then decrypts the data using the corresponding private key.
Public Key Infrastructure (PKI)	The standards and services that facilitate the use of public-key cryptography and certificates in a networked environment.
RiskFort	RiskFort provides a mechanism to evaluate the risk of a given transaction.
Risk Advice	An action (ALLOW , ALERT , DENY , INCREASEAUTH) suggested by RiskFort to the calling application, after evaluating the risk of an transaction.
RiskFort Native Protocol	Arcot proprietary protocol for communication between RiskFort Server, its components and Administration Console.
Risk Score	RiskFort announces a score depending on the evaluation result. The score can be a number from 0 through 100. The greater the number, the higher the risk.
Scoring Callout	Callout that runs after scoring by RiskFort's Scoring Engine and contains custom scoring logic to modify final Risk Score .

Scoring Engine	Component of RiskFort Server that collects Risk Scores from individual Evaluation Rules and processes them in the order of the scoring precedence.
Scoring Rule	Last Rule that receives execution results of all other configured rules and returns the final Risk Score and Risk Advice .
Server Management Protocol	Arcot proprietary protocol for starting and shutting down the RiskFort Server.
Secure Sockets Layer (SSL)	Protocol for managing the security of a message transmission on public networks.
Terminating Rule	The rule that alone determines overall Risk Score .
Transmission Control Protocol (TCP)	Internet protocol for guaranteed transmission of data. It sends data unencrypted.
Trusted Aggregator	Aggregator “trusted” to the organization and, therefore, excluded from future risk assessments.
Trusted IP Address	IP address that is “trusted” and, therefore, excluded from future risk evaluations.
Two-Way SSL	Both, client application and the server application verify each other’s identity (by presenting respective Digital Certificate) before the SSL session is established.
UserID/Password	One of the credential issued to the user during enrollment.
User Velocity	Number of transactions from the same user within a specified time.
Velocity Check	See Device Velocity and User Velocity .
Zone Hopping	Successive transactions (from same user) separated by a distance of more than what a reasonable user-speed can achieve.

Index

A

active data [103](#)

Add-On Rules

 Rule Type [61](#)

 Custom [66](#)

 Pre-Existing [61](#)

Add-On rules [58](#)

Administration Console [1](#)

administrative user

 Global Administrator [9](#)

 Master Administrator [8](#)

 Organization Administrator [9](#)

 User Administrator [10](#)

Advice [117](#)

aggregators [85](#)

annotation string [59](#)

Arcot RiskFort Data Upload Tool [309](#)

arrfserver [307](#)

B

BA [32](#)

base elements [183](#)

Basic Authentication [32](#)

C

Callout [127](#)

 Evaluation [59](#)

 Scoring [59](#)

Case Management [226](#)

 case [226](#)

case management role

 Customer Support Representative [233](#)

 Fraud Analyst [234](#)

Queue Manager [234](#)

configuration

 negative IP address list [103](#)

 migrating to production [121](#), [141](#)

 negative country list [103](#)

 protocol setup [118](#), [132](#)

 trusted aggregators [85](#)

Connection Timeout [136](#)

CSR [233](#)

D

DBUtil

 inserting userID and password [299](#)

 options [300](#)

Default Organization [29](#)

Derived Data [65](#)

E

enrollment [213](#)

Evaluation Callout [59](#)

Exception user [57](#)

Exception User List [57](#)

Extensible elements [183](#)

F

features

 sample Risk Advice matrix [118](#)

I

instance [1](#)

Intended Audience [xiii](#)

L

List Data [64](#)

log

severity level [319](#)

log level [319](#)

M

Mapping Data [65](#)

master key [298](#)

modifier string [59](#)

multi-tenant architecture [1](#)

N

Negative Country list [100](#)

Negative IP address list [93](#)

O

organization [147](#)

P

preferred organization [199](#)

R

Read Timeout [136](#)

Risk Advice [117](#)

Risk Advice Matrix [118](#)

Risk Score [117](#)

RiskFort data

active data [122](#)

proposed data [121](#)

RiskFort Predictive Model [62](#)

Roles [4](#)

administrative user [5](#)

Custom roles [14](#), [36](#)

user [5](#)

Rule types

Evaluation

Standalone

Add-On [58](#)

Built-in [57](#)

Scoring [59](#)

terminating [57](#)

ruleset [78](#)

S

scope [7](#)

Score [117](#)

Scoring Callout [59](#), [131](#)

Scoring Rules [59](#)

staging data [103](#)

Supervisor [234](#)

system administration tools [297](#)

arrfadmin [302](#)

DBUtil [297](#)

system adminsitration tools

aradmin [302](#)

dbutil [297](#)

T

terminating rules [57](#)

third party [ii](#)

trust store [47](#)

Trusted IP address list [81](#)

U

UDS [25](#)

user creation mode [112](#)

explicit [112](#)

implicit [112](#)

User Data Service [25](#)

V

Velocity check

Device Velocity [106](#)

User Velocity [103](#)

Z

Zone hopping [109](#)