

Arcot RiskFort™ Administration Guide

Version 1.7



455 West Maude Avenue, Sunnyvale, CA 94085

Arcot RiskFort Administration Guide
Version 1.7
March 2009
Part Number: ARF01-002DC-17000

Copyright © 2009 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®, and WebFort VAS® are registered trademarks of Arcot Systems, Inc. The Arcot logo™, the Authentication Authority tagline, ArcotID Client™, RegFort™, RiskFort™, SignFort™, and TransFort™ 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 third-party software used by Arcot RiskFort and related components are listed in the appendix “Third-Party Software Licenses” in the *RiskFort Installation and Deployment Guide*.

Contents

Preface	iii
Intended Audience	iii
Information Included in this Guide	iv
Related Publication	iv
Conventions Used in This Book	iv
Contacting Support	v
Chapter 1 Understanding the RiskFort Administration Console	1
Navigating the Administration Console	2
Understanding the Administrator Levels	4
Master Administrator	4
Global Administrator	5
Customer Support Representatives (CSRs)	5
Chapter 2 Getting Started with the Administration Console	7
Performing Basic Administrative Tasks	8
Enrolling Administrators	8
Logging In and Out of the Administration Console	9
Changing the Administrator Password	10
Managing Administrators	12
Creating Administrator Accounts	12
Creating a Global Administrator Account	12
Creating a CSR Account	15
Updating Administrator Accounts	18
Enabling or Disabling Administrator Accounts	20
Deleting Administrator Accounts	21
Administrative Privileges Summary	23

Chapter 3 Configuring RiskFort	25
Configuring Protocols	27
Configuring TLS Communication (Optional)	29
Configuring TLS for Communication Between WebFort Server and Administration Console	29
Configuring TLS for Server Management Protocol	31
Specifying the System Configuration	32
Configuring Trusted IP Addresses	34
Configuring Trusted Aggregators	38
Configuring Negative Country List	45
Configuring Negative IP Types	47
Configuring Negative IP Address List	49
Configuring Velocity Check	51
Configuring Zone Hopping Check	54
Configuring Scoring	57
Types of RiskFort Rules	57
Evaluation Rules	58
Scoring Rules	60
Scoring Configuration	60
Configuring Add-On Rules	63
Configuring Callouts	68
Migrating to Production	78
 Chapter 4 Working with RiskFort Reports	 81
Administrator Activity Reports	82
Administrator Activity Audit Reports	82
Authentication Activity Report	85
RiskFort Configuration Data Reports	87
RiskFort Trusted IP/Aggregator Report	87
RiskFort Negative IP Report	89
RiskFort Negative Country Report	90
RiskFort Exception User Report	91
RiskFort Add-On Rules Report	93
RiskFort Transaction Reports	95
Risk Advice Summary Report	95
Risk Evaluation Detail Activity Report	96
Exporting Reports to a File	100
 Chapter 5 Tools for System Administrators	 101
dbutil (RiskFort Database Tool)	102
Set Up the Master Key	102
Insert a Database User Name and Password	103
Use Additional dbutil Options	104
arversion (RiskFort Modules Version Display Tool)	105

aradmin (RiskFort Server Refresh and Shutdown Tool)	106
Configuring for TLS-Based Communication	107
Edit arcotcommon.ini	107
Configure Server Management Protocol	108
arrfupload (Arcot RiskFort Data Upload Tool)	109
riskfortdataupload.ini	111
Appendix A Working with Sample Callouts	115
Deploying Sample Callouts	116
On Windows	116
On UNIX-Based Platforms	116
Configuring RiskFort Server to Communicate With Sample Callouts	117
Using Sample Callout	119
Appendix B Glossary	121
Index	125

Preface

Welcome to the Arcot RiskFort Administration Guide. This guide discusses the following topics:

- RiskFort Administration Console
- RiskFort administrator hierarchy
- RiskFort configuration and global settings
- RiskFort reports
- RiskFort system administration tools

Intended Audience

This manual is intended for administrators of Arcot RiskFort. It describes how to use the RiskFort Administration Console to perform the typical administrative tasks relating to maintenance, provisioning, updating, monitoring performance, and modifications of RiskFort and its components.

This guide is intended for users who are experienced with:

- Running operating system-based administration operations, such as creating users and groups, adding users to groups, setting group policies and user rights
- Applicable Oracle and/or MS SQL databases
- Application servers
- Web server administration

Information Included in this Guide

This guide is organized as follows:

- **Chapter 1, “Understanding the RiskFort Administration Console”**, introduces you to the RiskFort Administration Console interface and management hierarchy.
- **Chapter 2, “Getting Started with the Administration Console”**, describes the basic administrative tasks, such as enrolling administrators, logging in and out of the Administration Console, changing the administrator password. It also discusses the procedures for creating, updating, and deleting administrator accounts.
- **Chapter 3, “Configuring RiskFort”**, discusses how to configure RiskFort to meet your business needs.
- **Chapter 4, “Working with RiskFort Reports”**, discusses the various reports offered by RiskFort.
- **Chapter 5, “Tools for System Administrators”**, discusses the tools provided by RiskFort that system administrators can use to monitor and manage the system.
- **Appendix A, “Working with Sample Callouts”**, walks you through the steps to deploy the Sample Callout shipped with RiskFort.
- **Appendix B, “Glossary”**, lists the key terms related to RiskFort.

Related Publication

Other related publications are as follows:

<i>Arcot RiskFort Installation and Deployment Guide</i>	This guide provides information for installing and configuring RiskFort and its components.
---	---

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Click the Install button to install the product.
<i>Italic</i>	Key Words	First time log in to the <i>Administration Console</i> must be done using Master Admin credentials.
	Names of Publications	For more information, see the <i>Arcot RiskFort Administration Guide</i> .

Type	Usage	Example
	Emphasis	<i>Never</i> give anyone your password.
Cross reference	Links in the guide	Refer to the section Upgrading RiskFort for more information.
Fixed-width	Command-line input or output Code Samples Text File Content File and folder names	<pre># cd /opt/oracle/ ./riskfortserver start [arcot/db/primarydb] # The name of the data source as # defined in ODBC. Datasource.1=ArcotWebFortDatabase arcotcommon.ini</pre>

Contacting Support

If you need help, contact Arcot Support as follows:

Email	support@arcot.com
Web site	http://support.arcot.com

Chapter 1

Understanding the RiskFort Administration Console

Arcot RiskFort Administration Console (referred to as "Administration Console" later in the guide) is a Web-based, operation and system management tool. It provides administrative functions, such as server configurations, communication protocol set up, configuration of out-of-box rules or custom rules for risk evaluation, and report generation that enable you to perform the typical administrative tasks relating to provisioning, updating, monitoring performance, and maintenance of RiskFort and its components.

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

- [Navigating the Administration Console](#)
- [Understanding the Administrator Levels](#)

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

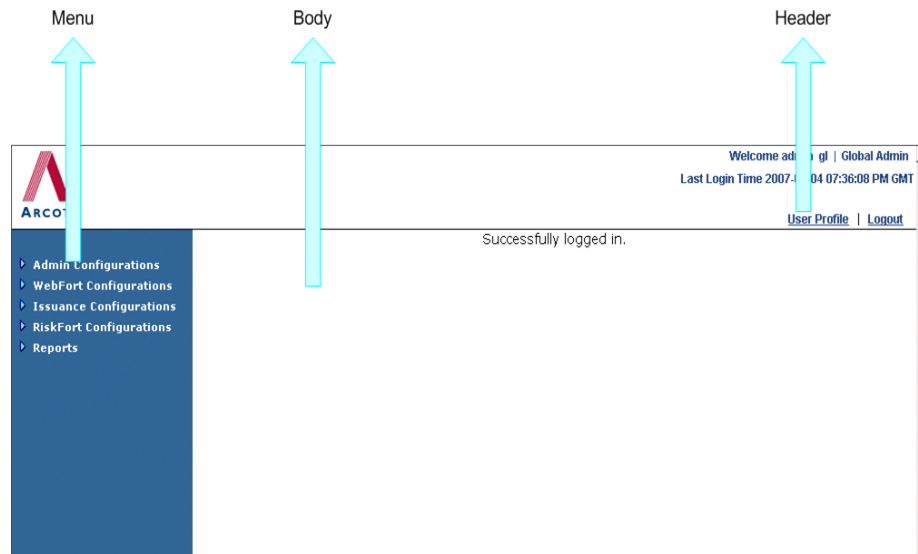
Navigating the Administration Console

The Administration Console provides a uniform user interface for all administrator levels (see “[Understanding the Administrator Levels](#),” for more information) supported by RiskFort. A typical Administrative screen can be divided into the following three frames:

- Header
- Menu
- Body

The following figure illustrates the placement of these frames in the Administration Console user interface.

Figure 1-1



The following table discusses the three-framed view of the Administration Console user interface.

Table 1-1 Administration Console User Interface

Frame	Description
Header	Displays login information (User Name, the last login date and time). The header displays the following links: • User Profile: Displays the logged-in administrator's profile. • Logout: Exits the Administration Console, when clicked.
Menu	Displays the configuration menu available to the current administrator.
Body	Displays the task page for the selected menu.

Understanding the Administrator Levels

RiskFort administrative functions are distributed among the following three levels of administrators:

- **Master Administrator**
- **Global Administrator**
- **Customer Support Representatives (CSRs)**

NOTE: RiskFort currently supports two user groups that are available at the end of a successful installation. These include GROUP2 (user group) and ADMINISTRATORS (administrators group).

The following sub-sections discuss each administrator role, and the relationship between them.

Master Administrator

Master Administrator (MA) is the highest level of administrator. The primary responsibilities of Master Administrator are to:

- Initialize the system after installation
- Create and manage Global Administrator accounts

At the end of the successful installation of Administration Console, you must log in for the first time as a Master Administrator using the following credentials:

- **User name:** *master_admin*
- **Password:** *master1234*

NOTE: Arcot strongly recommends that you change the password after the first login. Refer to the section, “[Changing the Administrator Password](#),” for more information.

NOTE: In case the Master Administrator account is locked, then contact Arcot Technical Support at support@arcot.com.

After you log in as Master Administrator for the first time, you must create Global Administrators.

As a Master Administrator, you can also view the activity logs of other administrators in the system.

Global Administrator

Global Administrator (GA) is the second level of administrator in the administrator hierarchy. The primary responsibilities of a GA include:

- Managing Customer Support Representatives (CSRs)
- Configuring the system
 - Setting up the communication protocol between different components of RiskFort
- Configuring risk evaluation rules and scores
 - Trusted aggregators and IP address lists
 - Negative country and IP list
 - Negative IP type list
 - Device and Velocity checks
 - Zone hopping check
- Enabling and disabling required rules
- Specifying the scoring priority
- Configuring
 - Add-On rules
 - Callouts
- Generating activity reports

GAs can also view and generate activity reports for CSR administrators assigned to them.

Customer Support Representatives (CSRs)

Also known as CSR Administrators, these administrators are responsible for user management operations and generating user activity reports in the system. CSRs can *only view* user reports.

CSR accounts can be created either by Global or Master Administrators.

Chapter 2

Getting Started with the Administration Console

Administrators are the main users of the Administration console. The primary responsibility of RiskFort administrators include:

- Creating and updating administrative accounts
- Configuring and updating rules and scores
- Setting up the communication protocols
- Migrating the changes to production

This chapter guides you through the steps for:

- [Performing Basic Administrative Tasks](#)
- [Managing Administrators](#)

NOTE: Advanced tasks, such as configuring rules and scoring, setting up the protocols, and making the configurations active are discussed in details in [Chapter 3, “Configuring RiskFort”](#).

The chapter also provides a summary of administrative privileges available to different administrators in the [“Administrative Privileges Summary”](#) section.

Performing Basic Administrative Tasks

All administrators can perform the following administrator-specific tasks:

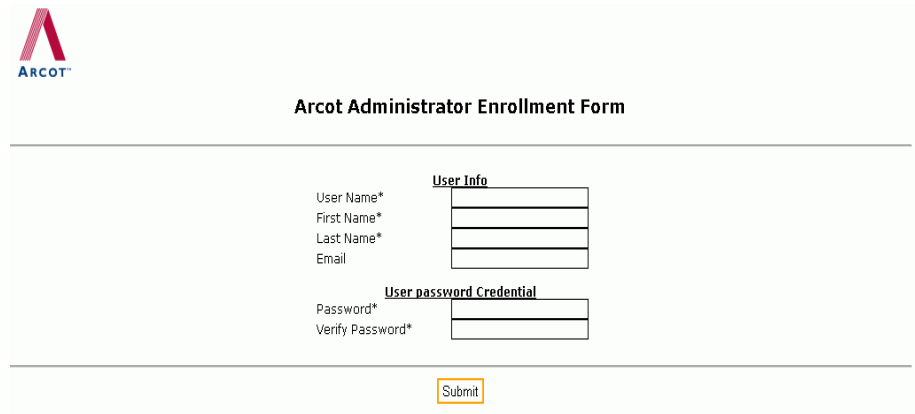
- [Enrolling Administrators](#)
- [Logging In and Out of the Administration Console](#)
- [Changing the Administrator Password](#)

Enrolling Administrators

Administrative users must enroll themselves and obtain credentials to log in and perform administrative tasks.

The following figure displays the administrator Enrollment Form page, used for the purpose of enrolling administrators.

Figure 2-1



The screenshot shows the 'Arcot Administrator Enrollment Form' page. At the top left is the Arcot logo. The title 'Arcot Administrator Enrollment Form' is centered. Below the title, the form is divided into two main sections: 'User Info' and 'User password Credential'. The 'User Info' section contains four input fields: 'User Name*', 'First Name*', 'Last Name*', and 'Email'. The 'User password Credential' section contains two input fields: 'Password*' and 'Verify Password*'. At the bottom right of the form is a 'Submit' button.

User Info	
User Name*	
First Name*	
Last Name*	
Email	

User password Credential	
Password*	
Verify Password*	

To enroll an administrative user, perform the following steps:

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

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

The Login page appears.

3. Click the **Register Now** link on the Login page.

The Arcot Administrator Enrollment Form page is displayed, as shown in [Figure 2-1](#).

4. Complete the enrollment form by entering the required details and click **Submit**.

NOTE: Fields marked with * are mandatory. **User Name** is not case sensitive.

After successful enrollment, you will be re-directed to the Administrator Login page in 5 seconds.

NOTE: Enrolled users can log in to the Administration Console *only if* they have been promoted as administrators.

Logging In and Out of the Administration Console

At the end of a successful installation, the Master Administrator account is available for login to the Administration Console. Use the following credentials to log in to the console:

- **User name:** *master_admin*
- **Password:** *master1234*

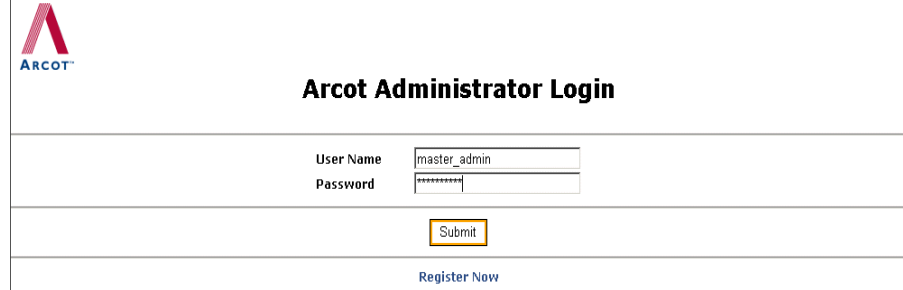
Subsequently, to create other administrator accounts, users *must* first enroll themselves. See “[Enrolling Administrators](#)” for more information on enrolling an administrative accounts.

To log in to the Administration Console, perform the following steps:

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

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

The Administrator Login page appears, as shown in the following figure.

Figure 2-2


The figure shows the Arcot Administrator Login page. At the top left is the Arcot logo. The title "Arcot Administrator Login" is centered. Below the title is a form with two input fields: "User Name" containing "master_admin" and "Password" containing "*****". A "Submit" button is below the password field. At the bottom, there is a "Register Now" link.

3. Enter the **User Name**, **Password** of the Master Administrator, and click **Submit**.

The Administration Console with the message "Successfully logged in" is displayed.

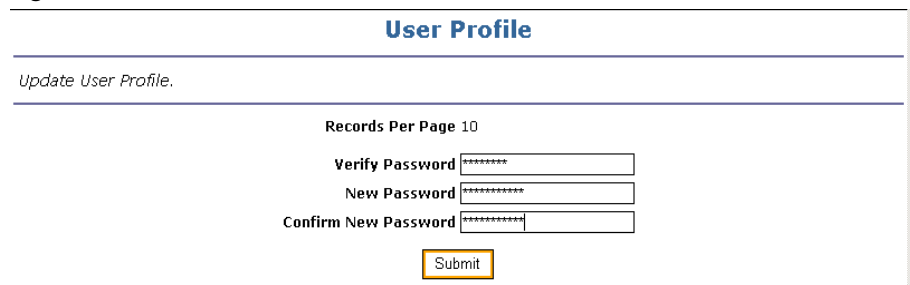
To log out of the Administration Console, click the **Logout** button. The Arcot Administrative Login page will be displayed.

Changing the Administrator Password

Administrators can change their password according to the policies of your organization.

NOTE: It is highly recommended that you change the Master Administrator password after logging in to the console for the first time.

Use the User Profile page, shown in the following figure, to change the administrator passwords.

Figure 2-3


The figure shows the User Profile page. The title "User Profile" is centered at the top. Below the title is a horizontal line, followed by the text "Update User Profile." Below this is another horizontal line. Underneath, there is a "Records Per Page 10" label. Then, there are three input fields: "Verify Password" with "*****", "New Password" with "*****", and "Confirm New Password" with "*****". A "Submit" button is at the bottom.

To change your administrator password, perform the following steps:

1. In the Administration Console, click the **User Profile** link.

The User Profile page is displayed, as shown in [Figure 2-3](#).

2. Enter the following information:
 - The current password in the **Verify Password** field.
 - The new password in the **New Password** field.
 - The new password again in the **Confirm New Password** field.
3. Click **Submit**.

A success message, indicating that the password is changed, is displayed.

Use this new password to subsequently log in to Administration Console.

Managing Administrators

This section discusses the following tasks related to managing administrators and their accounts:

- [Creating Administrator Accounts](#)
- [Updating Administrator Accounts](#)
- [Enabling or Disabling Administrator Accounts](#)
- [Deleting Administrator Accounts](#)

Creating Administrator Accounts

An administrator who belongs to one level can create other administrators who belong to a lower level in the administrator level. For example:

- Master Administrator can create all other types of administrators.
- Global Administrator accounts (GA) can create Customer Support Representative (CSR) accounts.

NOTE: For more information on the privileges available to administrators at each level, refer to the "[Administrative Privileges Summary](#)" section.

The hierarchical level of an administrator is determined by the administrative policy, which is associated while creating the administrator account.

This section discusses the steps to create the following administrator accounts:

- [Creating a Global Administrator Account](#)
- [Creating a CSR Account](#)

Creating a Global Administrator Account

To create a Global administrator account, perform the following steps:

1. Log in to the Administration Console as Master Administrator.
2. Under **Admin Configurations**, select the **Create Admin** option.

The User Search page appears, as shown in the following figure.

Figure 2-4

The screenshot shows the Arcot RiskFort Administration Console interface. At the top left is the Arcot logo. At the top right, it says "Welcome admin gl | Global Admin" and "Last Login Time 11/07/2007 15:50:43 PM GMT". Below this are links for "User Profile" and "Logout". On the left is a blue sidebar menu with the following items: "Admin Configurations" (expanded), "Create Admin", "Update Admin", "Delete Admin", "WebFort Configurations", "Issuance Configurations", "SignFort Configurations", "RiskFort Configurations", and "Reports". The main content area is titled "User Search" and contains the instruction "Display users based on Search Criteria." Below this is a search form with three input fields labeled "User Name", "First Name", and "Last Name". A "Search" button is located below the "Last Name" field.

3. Provide complete or partial details of the user and click the **Search** button.

A list of enrolled users matching the search criteria and who are not administrators is displayed.

4. Click the **User Name** link for the user you want to promote as an administrator.

The Create Admin page is displayed with the details of the user you selected, as shown in the following figure.

Figure 2-5

Create Admin

Create an administrator for the selected groups with the specified policy.

User Name	ALANJOHNSON	First Name Last Name	alan johnson	Group	ADMINISTRATORS
------------------	-------------	---------------------------------	-----------------	--------------	----------------

Policy Global Admin-Policy

Available Groups

ADMINISTRATORS
GROUP2

>

>>

<

<<

Selected Groups

Disable Admin ☐

Save
Cancel

5. To specify the level of the administrator, you must select the policy to be associated. Select the **Global Admin-Policy** option from the **Policy** drop-down list.
6. Select the group from the **Available Groups** list and click the > button to add the group to the **Selected Groups** list.

The **Available Groups** list displays all user groups who are under the administrative purview of Master Administrator.

The **Selected Groups** displays all user groups that will be under the administrative purview of the new administrator being created.

7. Click the **Save** button to complete the task.

The "Admin created successfully" message is displayed, as shown in the following figure.

Figure 2-6

Create Admin

Create an administrator for the selected groups with the specified policy.

Admin created successfully

User Name	ALANJOHNSON	First Name	alan	Group	ADMINISTRATORS
		Last Name	johnson		

Policy Global Admin Policy ▾

Available Groups

>

>>

<

<<

Selected Groups

ADMINISTRATORS
GROUP2

Disable Admin ☐

Save

Cancel

Creating a CSR Account

To create a CSR account, perform the following steps:

1. Log in to the Administration Console as Global Administrator.
2. Under **Admin Configurations**, select the **Create Admin** option.

The User Search page appears, as shown in the following figure.

Figure 2-7

The screenshot shows the Arcot RiskFort Administration Console interface. At the top left is the Arcot logo. At the top right, it says "Welcome admin gl | Global Admin" and "Last Login Time 11/07/2007 15:50:43 PM GMT". Below this are links for "User Profile" and "Logout". On the left is a blue sidebar menu with the following items: "Admin Configurations" (expanded), "Create Admin", "Update Admin", "Delete Admin", "WebFort Configurations", "Issuance Configurations", "SignFort Configurations", "RiskFort Configurations", and "Reports". The main content area is titled "User Search" and contains the instruction "Display users based on Search Criteria." Below this is a search form with four input fields labeled "User Name", "First Name", "Last Name", and "Last Name". A "Search" button is located below the "Last Name" field.

3. Provide complete or partial details of the user and click the **Search** button.

A list of enrolled users matching the search criteria and who are not administrators is displayed.

4. Click the **User Name** link for the user you want to promote as an administrator.

The Create Admin page is displayed with the details of the user you selected, as shown in the following figure.

Figure 2-8

Create Admin					
Create an administrator for the selected groups with the specified policy.					
User Name	JACK	First Name	jack	Group	ADMINISTRATORS
		Last Name	jack		
Policy	CSR Policy				
Available Groups 		> >> < << Selected Groups ADMINISTRATORS GROUP2			
Disable Admin	☐				
		Save Cancel			

- To specify the level of the administrator, you must select the policy to be associated. Select the **CSR Policy** option from the **Policy** drop-down list.
- Select the group from the **Available Groups** list and click the > button to add the group to the **Selected Groups** list.

The **Available Groups** list displays all user groups who are under the administrative purview of Global Administrator.

The **Selected Groups** displays the group that will be under the administrative purview of the new administrator being created.

- Click the **Save** button to complete the task.

The "Admin created successfully" message is displayed, as shown in the following figure.

Figure 2-9

Create Admin

Create an administrator for the selected groups with the specified policy.

Admin created successfully

User Name	JACK	First Name	jack	Group	ADMINISTRATORS
		Last Name	jack		

Policy CSR Policy

Available Groups

>

>>

<

<<

Selected Groups

ADMINISTRATORS
GROUP2

Disable Admin ☐

Updating Administrator Accounts

When you need to change the group(s) assigned to an administrator, you use the Update Admin page, shown in [Figure 2-10](#).

NOTE: RiskFort currently supports two user groups that are available at a end of successful installation. These include GROUP2 (user group) and ADMINISTRATORS (administrators group).

Figure 2-10

Update Admin

Update an administrator with the selected groups.

User Name	ALANJOHNSON	First Name	alan	Group	ADMINISTRATORS
		Last Name	johnson		
		Policy:	Global Admin Policy		

Available Groups

GROUP2

>

>>

<

<<

Selected Groups

ADMINISTRATORS

Disable Admin ☐

Update

Cancel

To update an administrator account, perform the following steps:

1. Log in to the Administration Console by using Global Administrator credentials.
2. Under **Admin Configurations**, select the **Update Admin** option.

The User Search page is displayed.

3. Provide complete or a partial user details on the User Search page and click **Search**.
4. A list of administrators matching the search criteria is displayed. Click the **User Name** whose account has to be updated.

The Update Admin page is displayed with the user name you selected.

5. Make the required changes and click **Update**.

The "Admin updated successfully" message is displayed.

Enabling or Disabling Administrator Accounts

Sometimes you might need to disable an existing administrator account. For example, an administrative user might leave the organization or go on an extended leave of absence. When you disable an account, you lock the administrator out of the system temporarily until you enable the account again.

Similarly, sometimes you might need to enable a locked administrative account. For example, when an administrative user returns from an extended leave of absence. By enabling an account, you allow the user who could not previously log in to access the system again.

You use the Update Admin page, shown in the following figure, to enable or disable an administrator account.

NOTE: Currently only the group(s) assigned to an administrator can be changed by using the **Disable Admin** option on the Update Admin page.

Figure 2-11

Update Admin

Update an administrator with the selected groups.

User Name	ALANJOHNSON	First Name	alan	Group	ADMINISTRATORS
		Last Name	johnson		
		Policy:	Global Admin Policy		

Available Groups

GROUP2

>

>>

<

<<

Selected Groups

ADMINISTRATORS

Disable Admin ☒

Update

Cancel

To update an administrator account, perform the following steps:

1. Log in to the Administration Console by using Global Administrator credentials.

2. Under **Admin Configurations**, select the **Update Admin** option.

The User Search page is displayed.

3. Provide complete or a partial user details on the User Search page and click **Search**.
4. A list of administrators matching the search criteria is displayed. Click the **User Name** whose account needs to be updated.

The Update Admin page is displayed with the user name you selected.

5. Enable or disable the selected administrator account.

If the user account that you selected is currently enabled, then to disable the account, select the **Disable Admin** option. However, if the selected user account is disabled, then clear the **Disable Admin** option to enable the account.

NOTE: When an administrator account is created, it is enabled by default.

6. Click **Update** to reflect the change.

The "Admin updated successfully" message is displayed.

NOTE: If an administrator whose account has been disabled tries to log in, an error message will be displayed.

Deleting Administrator Accounts

Sometime, you might need to delete an existing administrator account. For example, when an administrative user leaves the organization. When you delete an account, the user can no longer log in to the Administration Console. However, the user account and credentials are *not* removed from the system.

You must use the Delete Admin page, as shown in the following figure, to delete an administrative account.

Figure 2-12

Delete Admin

Delete the selected administrator.

User Name	ALANJOHNSON	First Name	alan	Group	ADMINISTRATORS
		Last Name	johnson		
		Policy:	Global Admin Policy		

Groups

ADMINISTRATORS
GROUP2

Disable Admin ☐

Delete Cancel

To delete an administrator account, perform the following steps:

1. Log in to the Administration Console by using Global Administrator credentials.
2. Under **Admin Configurations**, select the **Delete Admin** option.

The User Search page is displayed.

3. Provide complete or partial details of the user on the User Search page and click **Search**.
4. A list of administrators matching the search criteria is displayed. Click the **User Name** whose account has to be deleted.

The Delete Admin page is displayed with the user name you selected.

5. Click **Delete**.

The "Admin deleted successfully" message is displayed.

NOTE: After deleting an administrator, the user name will still be present in the list of enrolled users. You can create the administrator account later again, if required.

Administrative Privileges Summary

Table 2-1 summarizes the privileges available to the supported three levels of administrators.

The column name acronyms used in the following table are:

- Master Administrator --> **MA**
- Global Administrator --> **GA**
- CSR Administrator --> **CSR**

NOTE: The ✓ sign indicates the actions that are available to the specified level of administrator.

Table 2-1 Administrative Privileges Summary

Feature	Action	MA	GA	CSR
Administrator Account Management	Create GA Accounts	✓		
	Update GA Accounts	✓		
	Delete GA Accounts	✓		
	Create CSR Accounts	✓	✓	
	Update CSR Accounts	✓	✓	
	Delete CSR Accounts	✓	✓	

Table 2-1 Administrative Privileges Summary

Feature	Action	MA	GA	CSR
RiskFort Configurations	Protocol Setup		✓	
	Trusted IP Setup		✓	
	Trusted Aggregator Setup		✓	
	Negative IP Types		✓	
	Negative IP Address		✓	
	Update Negative Country List		✓	
	Velocity Check		✓	
	Zone Hopping Check		✓	
	Scoring Configuration		✓	
	Add-On Rules Configuration		✓	
	Callout Configuration		✓	
	System Configuration		✓	
	Migrate to Production		✓	
Reports	Administrator Activity Audit Report	✓	✓	
	RiskFort Add-On Rules Report		✓	
	RiskFort Trusted IP/Aggregator Report		✓	
	RiskFort Negative IP Report		✓	
	RiskFort Negative Country Report		✓	
	RiskFort Exception User Report		✓	✓
	Risk Advice Summary Report		✓	✓
	Risk Evaluation Detail Activity Report		✓	✓

Chapter 3

Configuring RiskFort

This chapter describes how to configure RiskFort to meet your business requirements:

- [Configuring Protocols](#)
- [Specifying the System Configuration](#)
- [Configuring Trusted IP Addresses](#)
- [Configuring Trusted Aggregators](#)
- [Configuring Negative Country List](#)
- [Configuring Negative IP Types](#)
- [Configuring Negative IP Address List](#)
- [Configuring Velocity Check](#)
- [Configuring Zone Hopping Check](#)
- [Configuring Scoring](#)
- [Configuring Add-On Rules](#)
- [Configuring Callouts](#)
- [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, [“Administrative Privileges Summary.”](#)

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.

Configuring Protocols

Administration Console must be configured for enabling communication between RiskFort Server and its components and between Administration Console and the WebFort Server. The port on which the server listens for each protocol can be configured using the RiskFort Protocol Setup page. These protocols are:

- **Server Management**

This protocol is used for server management tools that control activities, such as starting and shutting down the server.

See [Chapter 5, “Tools for System Administrators”](#) for detailed information on RiskFort server administration tools controlled by the Server Management protocol.

- **RiskFort Native**

This is Arcot’s proprietary binary protocol and is used for communication between RiskFort Server and its components (Java and Web Services APIs).

- **Issuance**

This protocol is used by RiskFort Server for issuance-related activities, such as creating or updating users in RiskFort database.

The following figure shows the RiskFort Protocol Setup page.

Figure 3-1

Welcome Admin | Global | Global Admin
Last Login Time 01/06/2009 11:43:53 AM GMT
[User Profile](#) | [Logout](#)

RiskFort Protocol Setup

Update RiskFort protocol details. If you are using SSL/TLS 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(s) are restarted.

Enable	Protocol	Port Number	Transport Security	SSL/TLS Certificate Details	
☒	Server Management	7980	TCP		Save
☒	RiskFort Native	7680	TCP		Save
☒	RiskFort Issuance	7690	TCP		Save

The following table discusses the fields in the RiskFort Setup page:

Table 3-1 RiskFort Setup Page Fields

Page Field	Description
Protocol	Specify the protocol for transactions. RiskFort supports the following protocols: • Server Management: This protocol is used to manage RiskFort Server. • RiskFort Native: This is a proprietary binary protocol supported by RiskFort for communication between its components. • Issuance: This protocol is used to manage users in RiskFort database. Use the check box in the Enable column, to enable the protocol.
Port Number	Enter the port number where the RiskFort services is available. The following are the default port numbers for RiskFort protocols: • Server Management: 7980 • RiskFort Native: 7680 • Issuance: 7690
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. • TLS: Transport Layer Security (TLS) provides higher security for transactions, because it encrypts and decrypts data that is being transmitted. See “Configuring TLS Communication (Optional),” for more information if you select TLS.
SSL/TLS Certificate Details	Specify the certificate chain that is used by the TLS transport security mode. Upload the Certificate Chain and Private Key of the certificate using the respective Browse buttons in the corresponding fields.

To set up a protocol, perform the following tasks:

1. Under **RiskFort Configurations** from the side-bar menu, select **Protocol Setup**.
The RiskFort Protocol Setup page appears, as shown in [Figure 3-1](#).
2. Select and enable the required protocol:
 - a. Select the corresponding check box in the **Enable** column to enable a protocol.

- b. Specify the **Port Number** for the enabled protocol.
- c. Specify the **Transport Security Mode**. This can be TCP (default) or TLS.
- d. If you selected TLS in the preceding step, specify the certificate chain that is used by the TLS transport security mode.

Upload the **Certificate Chain** and **Private Key** of the certificate chain by using the respective **Browse** buttons in the corresponding fields.

IMPORTANT: The certificates in the chain must follow the Leaf certificate --> Intermediate CA certificates --> Root certificate hierarchy.

- e. Click the **Save** button to save the changes.

The "Protocol information updated successfully." message is displayed.

NOTE: You must restart RiskFort Server for the changes to be effective.

3. Restart the RiskFort Server for the changes to take effect.

Configuring TLS Communication (Optional)

Administration Console is dependent on WebFort Server for authentication of administrative users. See section, "WebFort Basic Installation" in *Arcot RiskFort Installation and Deployment Guide* for more information on this.

By default, Administration Console uses Transmission Control Protocol (TCP) to communicate with WebFort Server. However, TCP is vulnerable to spoofing and man-in-the-middle attacks. To ensure secure communication between APIs and RiskFort Server and between Administration Console and WebFort Server, you can configure RiskFort Native and Server Management protocols to TLS (Transport Layer Security).

Configuring TLS for Communication Between WebFort Server and Administration Console

To configure TLS-based communication between Administration Console and WebFort Server:

1. Under **WebFort Configurations** from the side-bar menu, select **Protocol Setup**.

The WebFort Protocol Setup page appears, as shown in the following figure.

Figure 3-2

WebFort Protocol Setup

Update WebFort protocol details. If you are using SSL/TLS security, both the Certificate Chain and the Private Key must be uploaded in PEM format. The changes made using this screen are not active until the WebFort server(s) are restarted.

WebFort Network Protocols

Enable	Protocol	Port Number	Transport Security	SSL/TLS Certificate Details	
☒	WebFort Native	9742	TCP	Issuer Subject Valid From Valid Until ICN=SignfortCA EMAILADDRESS=webfort-india@arcot.com, CN=C=IN, OU=WEBFORT, O=ARCOT SYSTEMS, L=BANGALORE, ST=KARNATAKA, C=IN 03/17/2009 06:33:36 03/17/2009 06:43:36	Save
☒	WebFort ASPP	9741	TCP		Save
☒	WebFort RADIUS	1812	UDP		Save
☒	Server Management	9744	TCP		Save

2. Configure the **WebFort Native** protocol as follows:

- f. In the **Enable** column, ensure that the box corresponding to **WebFort Native** is selected.
- g. In the **Transport Security** column, select **TLS** from the drop-down list.
- h. In the **SSL/TLS Certificate Details** column:

- I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the CA certificate chain of the server.

IMPORTANT: The certificates in the chain must follow the Leaf certificate --> Intermediate CA certificates --> Root certificate hierarchy.

- II. Click **Browse** against **Private Key** to navigate to the appropriate location and upload the corresponding private key of the certificate chain.

NOTE: The certificate chain and the private key, both *must* be in . PEM format. In addition, the associated private key must be un-encrypted. If the private key is in . PEM format and encrypted, then the Administration Console will display an error message.

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

3. Configure the **adminserver.ini** file as follows:

- a. Navigate to the following location:

On Windows:

<install_location>\Arcot Systems\conf\

**On UNIX
Platforms:**

`<install_location>/arcot/conf/`

- b. Open the `adminserver.ini` file in an editor window.
 - c. In the `[arcot/admin/authconfig]` section, set the following parameters:
 - `transport=TLS` (By default, this parameter is set to TCP.)
 - `server.CACert=<absolute_path_of_Root_Certificate>`
 - d. Save the changes and close the file.
4. Restart WebFort Server.
 5. Restart the application server.

Configuring TLS for Server Management Protocol

Refer to “[Configuring for TLS-Based Communication](#)” on page 107 for detailed instruction to configure RiskFort **Server Management** protocol for TLS.

Specifying the System Configuration

User Creation Modes

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

- **Explicit**

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 Unknown User Rule ("[Types of RiskFort Rules](#)" on page 57) will match resulting in the **ALERT** risk advice.

- **Implicit**

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 match the User Unknown 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 "User Unknown Rule" will not match.

Machine FingerPrint (MFP)

To develop a risk profile in real time, and then generate a corresponding Risk Score and Advice, RiskFort collects the following categories of information from the end-user device (that is being used by the user for the current transaction):

- 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".

Use the System Configuration page to specify the user creation mode and the MFP match threshold.

Figure 3-3

Welcome Admin Global | Global Admin
Last Login Time
User Profile | Logout

System Configuration

Specify the mode in which users will be created in RiskFort and the threshold percentage at which Machine FingerPrint (MFP) will match.

1. User Creation Mode: If you select the "Implicit" option, then new users (who do not exist in the RiskFort database) will be automatically created during risk evaluation. However if you select the "Explicit" option, then your application must call the `createUser()` API to create the user in the RiskFort database.
2. Machine FingerPrint (MFP) Threshold %: If the MFP match percentage is more than this value, only then it will be considered a match.

Note: The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:

1. Migrate to Production
2. Refresh the RiskFort Server Cache

	Default	Active	Proposed
User Creation Mode:	Explicit	Implicit	☐ Implicit ☒ Explicit
Machine FingerPrint (MFP) Threshold %:	50	90	77

Save

To specify the user creation mode and the MFP threshold percentage, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **System Configuration**.

The System Configuration page is displayed, as shown in [Figure 3-3](#).

2. Under the **Proposed** column, specify the required mode for **User Creation Mode**.
3. Under the **Proposed** column, specify the appropriate value for **Machine FingerPrint (MFP) Threshold %**.
4. Click **Save** 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”](#) for instructions to do so.

6. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the `aradmin <server_ip> <server_port> -r` command.

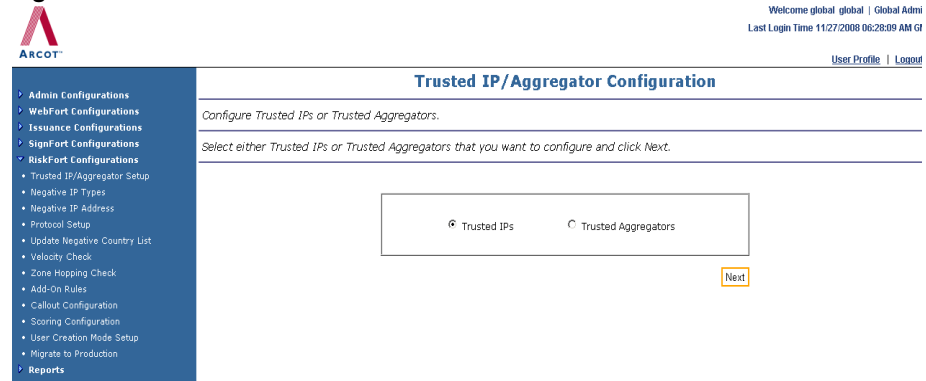
Configuring Trusted IP Addresses

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 assign them a low risk score and the ALLOW advice.

You can use the Administration Console to configure the Trusted IP address list. Use the Trusted IP/Aggregator Setup page, shown in the following figure, to perform the following tasks related to trusted IP addresses and ranges:

- Adding a Trusted IP Address or Range
- Updating a Trusted IP Address or Range
- Deleting a Trusted IP Address or Range

Figure 3-4



Adding a Trusted IP Address or Range

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

1. Under **RiskFort Configurations** on the side-bar menu, select **Trusted IP/Aggregator Setup**.

The Trusted IP/Aggregator Configuration page is displayed, as shown in [Figure 3-4](#).

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

The Trusted IP Configuration page, shown in [Figure 3-5](#), appears.

Figure 3-5

Welcome global | global | Global Admin
Last Login Time 11/27/2008 06:28:09 AM GMT
[User Profile](#) | [Logout](#)

Trusted IP Configuration

Configure Trusted IPs.

Note: The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:
1. Migrate to Production
2. Refresh the RiskFort Server Cache

Add Trusted IP

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

[Save Trusted IP](#)

Trusted IP List

	IP Address	Subnet Mask	End IP Address
☐			

[Delete](#) [Update](#)

3. On the Trusted IP Configuration page, in the **Add Trusted IP** section:
 - a. Specify the required IP address in the **IP Address** field.
 - b. 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 range of IP addresses to be added to the Trusted IP List.
 4. Click the **Save Trusted IP** button to add the IP address or range to the Trusted IP List.
- 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**” for instructions to do so.
 6. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

Updating a Trusted IP Address or Range

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

1. Under **RiskFort Configurations** on the side-bar menu, select **Trusted IP/Aggregator Setup**.

The Trusted IP/Aggregator Configuration page is displayed, as shown in [Figure 3-4](#).

2. Select **Trusted IPs** option and click **Next**.

The Trusted IP Configuration page, shown in the [Figure 3-5](#), appears.

3. On the Trusted IP Configuration page, select the required IP addresses or ranges in the **Trusted IP List** section.
4. Make the required changes.
5. Click **Update** to update the changes that you made.

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](#)” for instructions to do so.

7. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:

- a. Navigate to the following directory:

```
<install_location>\Arcot Systems\bin\
```

On Windows:

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

Deleting a Trusted IP Address or Range

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

1. Under **RiskFort Configurations** on the side-bar menu, select **Trusted IP/Aggregator Setup**.

The Trusted IP/Aggregator Configuration page is displayed, as shown in [Figure 3-4](#).

2. Select **Trusted IPs** option and click **Next**.

The Trusted IP Configuration page, shown in the [Figure 3-5](#), appears.

3. Select the required IP addresses or ranges that you want to delete in the **Trusted IP List** section.
4. Click **Delete** to delete the selected IP addresses or ranges.
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](#)” for instructions to do so.
6. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

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.

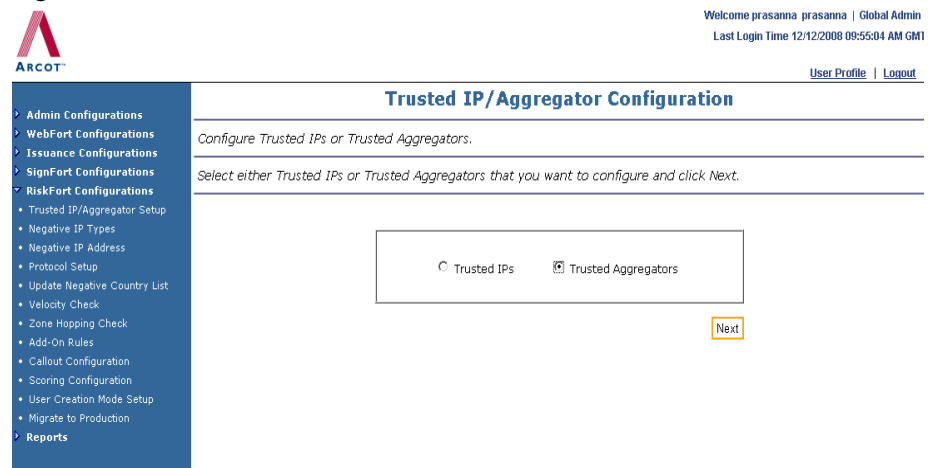
Transactions originating from (or routed through) aggregators “trusted” to the organization are considered low-risk. For this purpose, RiskFort provides the ability to configure a list of these aggregators so that all transactions originating from the aggregators’ IP addresses are assigned a low risk-score,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

Use the Trusted IP/Aggregator Setup page, shown in the following figure, to perform the following tasks related to trusted aggregators:

- Adding a Trusted Aggregator
- Updating a Trusted Aggregator
- Deleting a Trusted Aggregator

Figure 3-6



Adding a Trusted Aggregator

To add a trusted aggregator, perform the following tasks:

1. Under **RiskFort Configurations** on the side-bar menu, select **Trusted IP/Aggregator Setup**.

The Trusted IP/Aggregator Setup page is displayed, as shown in [Figure 3-6](#).

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

The Trusted Aggregator Setup page, shown in the following figure, appears.

Figure 3-7

The screenshot shows the Arcot RiskFort Admin console. The top right corner displays the user 'global' and the last login time '11/27/2008 06:28:09 AM GMT'. The sidebar on the left lists various configuration categories, with 'RiskFort Configurations' expanded to show 'Trusted IP/Aggregator Setup'. The main content area is titled 'Trusted Aggregator Setup' and contains a form with the following elements:

- A header instruction: 'Select an existing aggregator or specify the new aggregator name'.
- A note: 'Note: The changes made using this screen affect the staging data. Changes are not applicable until the staging data is made active using Migrate to Production and RiskFort servers are refreshed. See the Arcot RiskFort Manual for more details.'
- A 'Select existing Aggregator' dropdown menu currently showing '--Select--'.
- A 'New Aggregator' text input field.
- A yellow 'Next' button at the bottom right of the form.

3. Specify the name of the aggregator in the **New Aggregator** field and click **Next**.

The updated Trusted Aggregator Setup page, shown in the [Figure 3-7](#), appears.

Figure 3-8

Welcome global global | Global Admin
Last Login Time 11/27/2008 08:48:54 AM GMT

[User Profile](#) | [Logout](#)

Trusted Aggregator Setup

Update Aggregator ID will update the newly generated AID as primary AID in the database. This is an optional step required only if AID update is required. For updating IP address list click on next.

Note: The changes made using this screen affect the staging data. Changes are not applicable until the staging data is made active using Migrate to Production and RiskFort servers are refreshed. See the Arcot RiskFort Manual for more details.

Aggregator ID 1	gRn9wJ7x0MegyRI/nc1pjZx0ssgl4cMjqltq6w0Bo1x8tkizCXAS5ZhtxYyugE8
Aggregator ID 2	
Aggregator ID 3	

[Update Aggregator ID](#) [Next](#)

4. Click **Next** to continue.

The Trusted Aggregator Configuration page, as shown in the following figure, appears.

Figure 3-9

Welcome global global | Global Admin
Last Login Time 11/27/2008 08:48:54 AM GMT

[User Profile](#) | [Logout](#)

Trusted Aggregator Configuration

Configure IPs of Trusted Aggregator AG1

Note: The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:

1. Migrate to Production
2. Refresh the RiskFort Server Cache

Add Trusted IP

IP Address:									
Subnet Mask:									
End IP Address:									

[Save Trusted IP](#)

5. On the Trusted Aggregator Configuration page:
 - 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 Trusted IP List.
 - **End IP Address:** If you want to specify a range of IP addresses to be added to the Trusted Aggregator List.
- c. Click **Save Trusted IP** to add this IP address or range to the database.

The "Trusted IP added successfully." message is displayed, and the Trusted IP List section, as shown in the following figure, appears.

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

Figure 3-10

Welcome global global | Global Admin
Last Login Time 11/27/2008 08:46:54 AM GMT
[User Profile](#) | [Logout](#)

IP Address added successfully.

Trusted Aggregator Configuration

Configure IPs of Trusted Aggregator AG1

Note: The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:

1. Migrate to Production
2. Refresh the RiskFort Server Cache

Add Trusted IP

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

[Save Trusted IP](#)

Trusted IP List

	IP Address	Subnet Mask	End IP Address
☐	10 . 150 . 1 . 45	255 . 255 . 255 . 0	10 . 150 . 1 . 50

[Delete](#) [Update](#)

6. To make the changes active, you must migrate them to production.
Refer to “[Migrating to Production](#)” for instructions to do so.
7. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

`<install_location>\Arcot Systems\bin\`

**On UNIX
Platforms:**

`<install_location>/arcot/bin/`

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

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. The rotation duration can be decided based on 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, perform the following tasks:

1. Under **RiskFort Configurations** on the side-bar menu, select **Trusted IP/Aggregator Setup**.

The Trusted IP/Aggregator Setup page is displayed, as shown in [Figure 3-6](#).

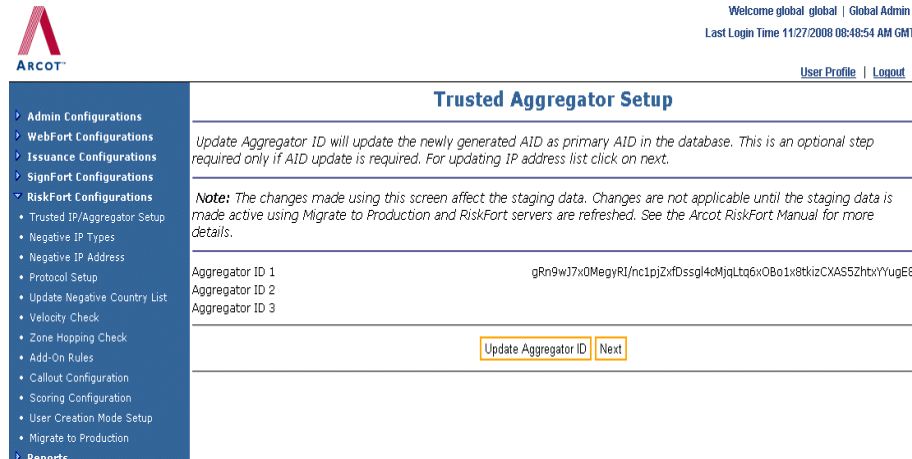
2. Select the **Trusted Aggregators** option and click **Next**.

The Trusted Aggregator Setup page, shown in [Figure 3-7](#), appears.

3. Specify an existing aggregator in the **Select existing Aggregator** field and click **Next**.

The updated Trusted Aggregator Setup page, shown in [Figure 3-11](#), with the Aggregator IDs for the selected aggregator appears.

Figure 3-11



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

The next empty Aggregator ID is displayed.

5. Click **Next** to continue.

The Trusted Aggregator Configuration page appears. This page enables you to update the IP address, range, or subnet mask for the specified IP address or range, if required.

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

The "Trusted IPs updated successfully." message is displayed.

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

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

Refer to **"Migrating to Production"** for instructions to do so.

9. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

Deleting a Trusted Aggregator

To delete a trusted aggregator, perform the following tasks:

1. Under **RiskFort Configurations** on the side-bar menu, select **Trusted IP/Aggregator Setup**.

The Trusted IP/Aggregator Setup page is displayed, as shown in [Figure 3-6](#).

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

The Trusted Aggregator Setup page, shown in [Figure 3-7](#), appears.

3. Specify an existing aggregator in the **Select existing Aggregator** field and click **Next**.

The Trusted Aggregator Configuration page ([Figure 3-8](#)) appears.

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 "Selected rows deleted successfully." message is displayed.

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](#)" for instructions to do so.

7. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:

- a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

On UNIX Platforms:

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

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.

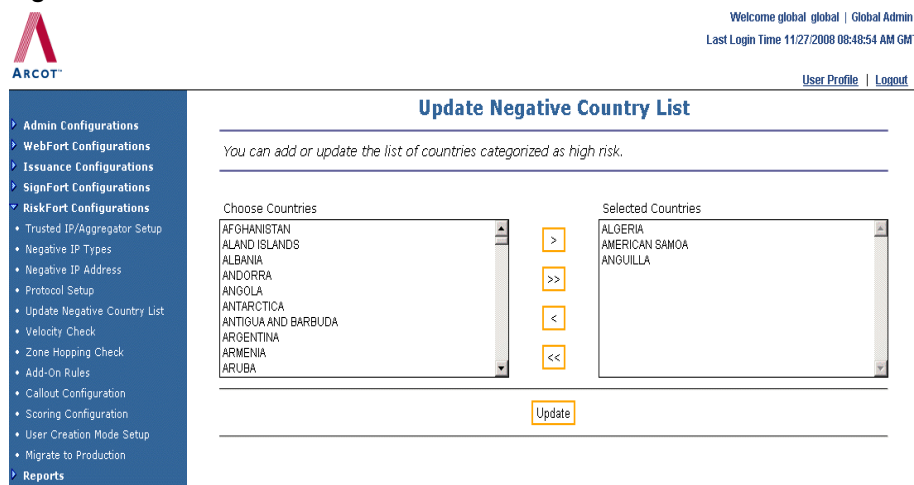
To know more about Quova and their services, go to:

<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 Update Negative Country List page, shown in the following figure, to add a country to the Negative Country list or remove a country from the list.

Figure 3-12



To update the Negative Country list, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Update Negative Country List**.

The Update Negative Country List page is displayed, as shown in [Figure 3-12](#).

2. Select the country you want to add from the **Choose Countries** list and add to the **Selected Countries** list.
3. 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.

4. Click **Update** to save the changes.

The "Negative Country List updated successfully." message is displayed.

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”](#) for instructions to do so.

6. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:

- a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

On UNIX Platforms:

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

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.

NOTE: You will 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 Address List” on page 49](#).

- **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 following figure, to configure the type of negative IP addresses applicable for your organization.

Figure 3-13

ARCOT

Last Login Time 11/27/2008 08:48:54 AM GMT

User Profile | Logout

Negative IP Types Configuration

Configure the Negative IP Types. The Negative IP Check Rule will use this configuration to determine if the IP of a transaction is negative or not.

The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:

1. Migrate to production
2. Refresh the RiskFort Server Cache using aradmin tool

IP Type	Default	Active	Proposed
Negative <i>Negative IP addresses that you have manually configured</i>	☒	☒	☒
Active <i>Anonymizers that have been tested positive within the last six months</i>	☒	☒	☒
Suspect <i>Anonymizers that have been tested positive within the last two years, but not the last six months</i>	☒	☒	☒
Private <i>Anonymous proxies not publicly accessible</i>	☒	☒	☒
Inactive <i>Anonymizers that have not been 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, perform the following tasks:

1. Under **RiskFort Configurations** on the side-bar menu, select **Negative IP Types**.
The Negative IP Types Configuration page, shown in [Figure 3-13](#), appears.
2. In the **Proposed** column, select the applicable types of negative IP addresses against each **IP Type**.
3. Click **Save** to save the changes.
The changes are yet not active, and not available to your end users.
4. To make the changes active, you must migrate them to production.
Refer to [“Migrating to Production”](#) for instructions to do so.
5. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

Configuring Negative IP Address List

Negative IP address list is a collection of IP addresses that have been the origin of known anonymizer proxies or fraudulent or malicious transactions in the past.

NOTE: This list is the source of the **Negative** category discussed in the “Configuring Negative IP Types” section.

Use the Add Negative IP Address page, as shown in the following figure, to configure the negative IP address list for your organization.

Figure 3-14

The screenshot displays the Arcot RiskFort web interface. On the left is a blue sidebar with a navigation menu. The top right of the page shows user information: 'Welcome global global | Global Admin' and 'Last Login Time 11/27/2008 08:48:54 AM GMT', with links for 'User Profile' and 'Logout'. The main content area is titled 'Add Negative IP Address' and includes a sub-header 'Add to a list of Negative IP Address Range.' Below this is a note: 'Note: The changes made using this screen affect the staging data. Changes are not applicable until the staging data is made active using Migrate to Production and RiskFort servers are refreshed. See the Arcot RiskFort Manual for more details.' The form contains four input fields: 'IP Address' (with a dotted placeholder), 'Subnet Mask' (selected with a radio button), 'End IP Address' (with a radio button), and 'Source'. At the bottom of the form are 'Add' and 'Delete' buttons.

To add or delete negative IP addresses, perform the following tasks:

1. Under **RiskFort Configurations** on the side-bar menu, select **Negative IP Address**.
The Add Negative IP Address page, shown in **Figure 3-14**, appears.
2. On the Add Negative IP Address page:
 - 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 Trusted IP List.
 - **End IP Address:** If you want to specify a range of IP addresses to be added to the Negative IP Address List.

- c. Specify the source (or vendor) of the negative IP address or range in the **Source** field.
3. Click one of the following buttons, as required:
 - **Add:** To add the specified IP address or range to the database.
 - **Delete:** 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.

4. To make the changes active, you must migrate them to production.
Refer to [“Migrating to Production”](#) for instructions to do so.
 5. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

Configuring Velocity Check

Velocity checks are of two types:

- *User Velocity rule* keeps a check on the number of transactions from a user within a specified period of time.
- *Device Velocity rule* keeps a check on the number of transactions from a device within a specified period of time.

The Velocity check rule 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.

- **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.

- **Time Interval**

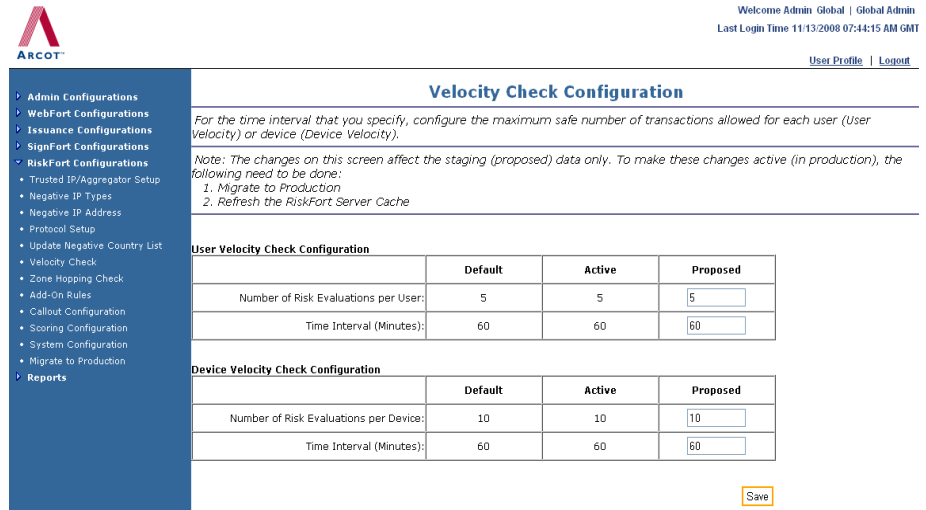
Denotes the time period (T) in which the number of transactions are being tracked.

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

Use the Velocity Check Configuration page, shown in the following figure, to do so.

NOTE: User Velocity Check and Device Velocity Check can be configured separately. You can choose to configure only User Velocity Check and not Device Velocity Check, or vice versa.

Figure 3-15



Welcome Admin Global | Global Admin
Last Login Time 11/13/2008 07:44:15 AM GMT
[User Profile](#) | [Logout](#)

Velocity Check Configuration

For the time interval that you specify, configure the maximum safe number of transactions allowed for each user (User Velocity) or device (Device Velocity).

Note: The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:

1. Migrate to Production
2. Refresh the RiskFort Server Cache

User Velocity Check Configuration

	Default	Active	Proposed
Number of Risk Evaluations per User:	5	5	5
Time Interval (Minutes):	60	60	60

Device Velocity Check Configuration

	Default	Active	Proposed
Number of Risk Evaluations per Device:	10	10	10
Time Interval (Minutes):	60	60	60

[Save](#)

To configure a Velocity rule, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Velocity Check**.
The Velocity Check Configuration page appears, as shown in [Figure 3-15](#).
2. In the **User Velocity Check Configuration** table, perform the following tasks to configure the User Velocity check:
 - a. If required, specify the **Proposed** value for the **Number of Risk Evaluations per User** 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 that as a risk, which will result in the matching of the User Velocity Check rule.
 - b. If required, specify the **Proposed** value for the **Time Interval** parameter.
3. In the **Device Velocity Check Configuration** table, perform the following tasks to configure the Device Velocity check:

- a. If required, specify the **Proposed** value for the **Number of Risk Evaluations per Device** 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 that as a risk, which will result in the matching of the User Velocity Check rule.

- b. Specify the **Proposed** value for the **Time Interval** parameter.

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

The "Velocity Check Configuration updated successfully." message is displayed.

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”](#) for instructions to do so.

6. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:

- a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

On UNIX Platforms:

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

Configuring Zone Hopping Check

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 check 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 Check Configuration page.

- **Maximum Variation in IP Address Location**

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 Variation in IP Address Location** field in the Zone Hopping Check Configuration page.

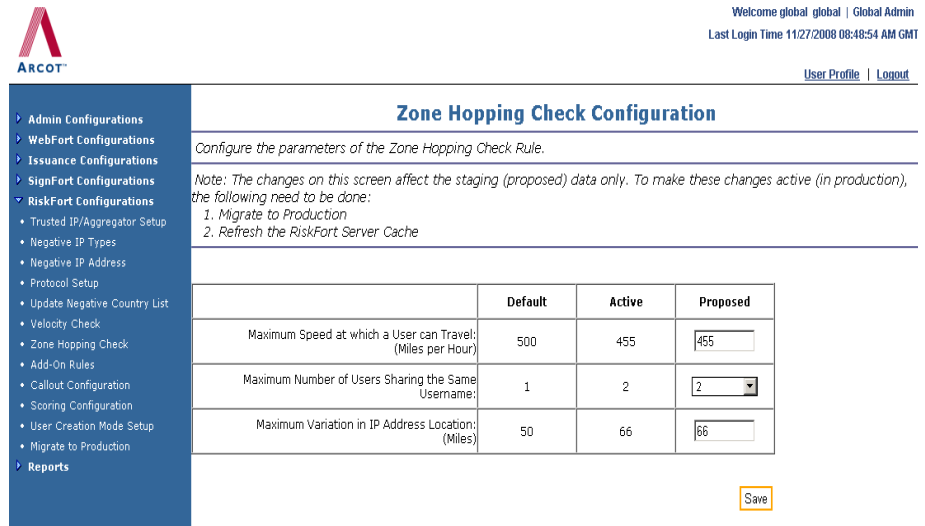
- **Maximum Number of Users Sharing the Same Username**

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 using the drop-down list against the **Maximum Number of Users Sharing the Same Username** field in the Zone Hopping Check Configuration page.

Use the Zone Hopping Check Configuration page, shown in the following figure, to configure this rule.

Figure 3-16



Zone Hopping Check Configuration

Configure the parameters of the Zone Hopping Check Rule.

Note: The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:

1. Migrate to Production
2. Refresh the RiskFort Server Cache

	Default	Active	Proposed
Maximum Speed at which a User can Travel: (Miles per Hour)	500	455	455
Maximum Number of Users Sharing the Same Username:	1	2	2
Maximum Variation in IP Address Location: (Miles)	50	66	66

[Save](#)

To configure the Zone Hopping rule, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Zone Hopping Check**.

The Zone Hopping Check Configuration page appears, as shown in [Figure 3-16](#).

2. Specify the **Proposed** value for the **Maximum Speed at which a User can Travel** parameter.
3. Specify the **Proposed** value for the **Maximum Number of Users Sharing the Same Username** parameter.
4. Specify the **Proposed** value for the **Maximum Variation in IP Address Location** parameter.
5. Click **Save** to save the changes.

The "Configuration updated successfully." message is displayed.

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”](#) for instructions to do so.

7. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

**On UNIX
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

Configuring Scoring

For each risk evaluation request from your application, RiskFort executes Evaluation rules to generate a *Risk Score* (or *Score*). This Score is a value from **0** through **100** that maps to a recommended *Risk Advice* (or *Advice*.)

The following table explains the mapping between the predefined score value ranges and corresponding Advice.

Table 3-2 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.

RiskFort uses a set of **Evaluation Rules** and **Scoring Rules** to evaluate a transaction and generate a Score and the corresponding Advice.

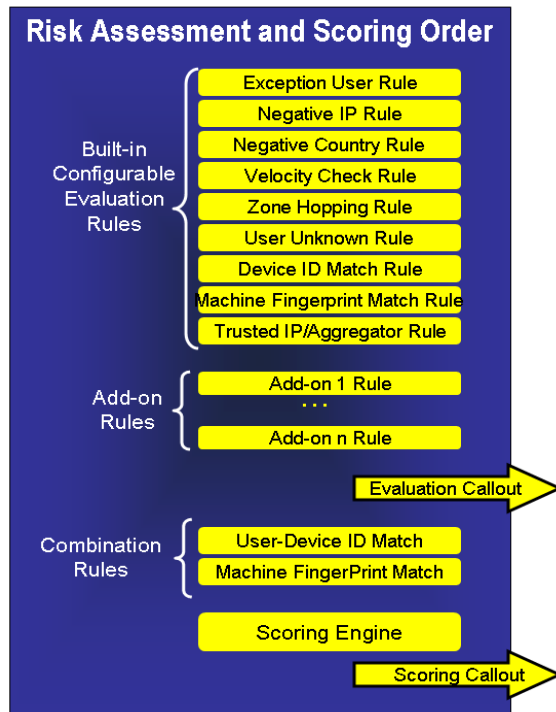
Types of RiskFort Rules

RiskFort rules can be categorized in to the following two broad categories:

- **Evaluation Rules**
- **Scoring Rules**

The following figure is a schematic diagram of RiskFort, with respect to various rules. The subtypes of all Evaluation and Scoring rules shown in **Figure 3-17** are discussed in subsections that follow the figure.

Figure 3-17



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:

- **Standalone 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.

Standalone rules include:

- **Built-in rules**

These are the out-of-the-box rules that are installed and deployed by default when you install RiskFort:

- **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 *Exception User List*, and are referred to as *exception users*. If found in the Exception User List, by default RiskFort returns a low Score and the ALLOW advice for transactions originating from exception users.)
- **Negative IP Check** (See “[Configuring Negative IP Address List](#)” on [page 49](#) for more information.)
- **Trusted IP/Aggregator Check** (See “[Configuring Trusted IP Addresses](#)” on [page 34](#) and “[Configuring Trusted Aggregators](#)” on [page 38](#) for more information.)
- **Negative Country Check** (See “[Configuring Velocity Check](#)” on [page 51](#) for more information.)
- **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.)
- **User Velocity Check** (See “[Configuring Velocity Check](#)” on [page 51](#) for more information.)
- **Device Velocity Check** (See “[Configuring Velocity Check](#)” on [page 51](#) for more information.)
- **Zone Hopping Check** (See “[Configuring Zone Hopping Check](#)” on [page 54](#) for more information.)

- **Add-On rules**

These include all additional rules shipped with RiskFort.

Unlike Built-in rules, these rules are installed, but not deployed automatically. See “[Configuring Add-On Rules](#)” on [page 63](#) for detailed information to do so.

- **Combination rules**

If the user (whose transaction is being evaluated) exists in the RiskFort database and if a corresponding User-Device association exists, then based on the User-Device association match and Machine FingerPrint match, following four combinations of rules 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

These are *non-terminating rules*. This implies that each of these rules is a combination of conditions that in conjunction with each other determine whether this rule has matched or not.

- **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. (See “[Configuring Callouts](#)” on page 68 for more information.) This Callout accepts results of all previous rules and extensible elements 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).

Scoring Rules

In addition to Evaluation rules, RiskFort also provides **Scoring Engine** (or **Scoring Rule**) 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. (See “[Configuring Callouts](#)” on page 68 for more information.)

Scoring Configuration

Use the Scoring Configuration page shown in following figure ([Figure 3-18](#)) for:

- Enabling or disabling rules
- Configuring the Risk Score and Scoring priority of rules

Figure 3-18



Welcome | Global Admin
 Last Login Time 12/12/2008 09:55:04 AM GMT
[User Profile](#) | [Logout](#)

- Admin Configurations
- WebFort Configurations
- Issuance Configurations
- Signfort Configurations
- RiskFort Configurations**
 - Trusted IP/Aggregator Setup
 - Negative IP Types
 - Negative IP Address
 - Protocol Setup
 - Update Negative Country List
 - Velocity Check
 - Zone Hopping Check
 - Add-On Rules
 - Callout Configuration
 - Scoring Configuration
 - User Creation Mode Setup
 - Migrate to Production
- Reports

Scoring Configuration

Configure the Risk Score and scoring priorities of rules. You can also enable or disable one or more rules, as required.

Note : The changes of the screen affect staging(proposed) data only. To make these changes active(in production), the following need to be done:
 1)Migrate to Production
 2)Refresh the RiskFort Server Cache

Risk Score	Advice
0-30	ALLOW
31-50	ALERT
51-70	INCREASEAUTH
71-100	DENY

Standalone Rules

RULE	DEFAULT			ACTIVE			PROPOSED			
	Enabled	Risk Score	Priority	Enabled	Risk Score	Priority	Enabled	Risk Score	Advice	Priority
Exception User Check	☒	30	10	☒	30	10	☒	30	ALLOW	↓
Negative IP Check	☒	100	20	☒	100	20	☒	100	DENY	↑ ↓
Negative Country Check	☒	100	30	☒	100	30	☒	100	DENY	↑ ↓
Trusted IP/Aggregator Check	☒	30	40	☒	30	40	☒	30	ALLOW	↑ ↓
Unknown User Check	☒	50	50	☒	50	50	☒	50	ALERT	↑ ↓
DeviceID Check	☒	65	60	☒	65	60	☒	65	INCREASEAUTH	↑ ↓
User Velocity Check	☒	65	70	☒	65	70	☒	65	INCREASEAUTH	↑ ↓
Device Velocity Check	☒	65	80	☒	65	80	☒	65	INCREASEAUTH	↑ ↓
Zone Hopping Check	☒	65	90	☒	65	90	☒	65	INCREASEAUTH	↑ ↓
Evaluation Callout	☐	N/A	N/A	☒	88	99	☐	88	DENY	↑

Combination Rules

RULE		DEFAULT	ACTIVE	PROPOSED	
User-DeviceID match	Machine FingerPrint match	Risk Score	Risk Score	Risk Score	Advice
YES	YES	10	10	10	ALLOW
NO	YES	65	65	65	INCREASEAUTH
YES	NO	65	65	65	INCREASEAUTH
NO	NO	65	65	65	INCREASEAUTH

Default Rule

	DEFAULT	ACTIVE	PROPOSED
Risk Score if Standalone or Combination Rules do not Match	30	30	30 ALLOW

Enable or Disable Scoring Callout

	ACTIVE	PROPOSED
Enable Scoring Callout:	☒	☐

[Save](#)

To enable or disable rules and to configure the Risk Score and Scoring priority of rules, perform the following steps:

- Under **RiskFort Configurations** on the side-bar menu, select **Scoring Configuration**.
The Scoring Configuration page appears, as shown in **Figure 3-18**.
- For each rule, in the **Proposed** column of the **Standalone Rules** table:
 - Select (to enable the rule) or clear (to disable the rule) the **Enabled** option.
 - Specify the required **Risk Score**.

- c. Click the Up (↑) arrow to increase the relative scoring priority or the Down arrow (↓) to decrease the scoring priority.
3. In the **PROPOSED** column of the **Combination Rules** table, for each rule specify the required **Risk Score**.
4. In the **PROPOSED** column of the **Default Rule** table, specify the required **Risk Score**.

RiskFort will use this value to generate the final Risk Score and Advice if none of the Standalone Rules or Combination Rules match.

5. In the **PROPOSED** column of the **Enable or Disable Scoring Callout** table, select (to enable the Scoring Callout) or clear (to disable the Scoring Callout) the provided option box.
6. Click **Save** to save the changes you made.
The changes 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](#)” for instructions to do so.
8. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
 - a. Navigate to the following directory:

On Windows:

```
<install_location>\Arcot Systems\bin\
```

On UNIX Platforms:

```
<install_location>/arcot/bin/
```

- b. Run the following command:
- ```
aradmin <server_ip> <server_port> -r
```

# Configuring Add-On Rules

In addition to the out-of-the-box evaluation rules that are shipped with RiskFort (see “[Configuring Scoring](#)” for more information), additional industry-specific rules are also supported. These terminating rules are referred to as *Add-On rules* and are run only *after* the out-of-the-box risk evaluation rules have finished executing.

**NOTE:** You must contact Arcot’s Professional Services unit at [services@arcot.com](mailto:services@arcot.com) to develop Add-On rules.

Add-On rules are implemented as .dll or .so library files, and typically use *Extensible elements*. These are additional name-value custom parameters that capture the real-time input from each transaction, and then are processed by the Add-On rule for successful risk evaluation.

After an Add-On rule is deployed, you *must* enable it by using the Scoring Configuration page ([Figure 3-18](#)) for it to take effect.

## Important Notes Related to Extensible Elements

- 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 extensible element.
- Extensible elements are programmatic elements, and *cannot* be configured by using the Administration Console.
- Extensible elements can be used by Add-On rules and Callouts. However, these elements cannot be used by out-of-box rules.
- An Add-On rule may not use any Extensible elements at all.

## Add-On Rule Example

Consider the following details of an Add-On rule that checks for transaction amounts more than \$20,000:

- **Rule Name:** High Amount Check
- **Description:** This rule checks for high transaction amounts that exceed the *parameter-value* (20,000) specified in the **Parameter Values** field.
- **Library Name:** highamountcheck.dll for Windows or highamountcheck.so for UNIX-based platforms
- **Mnemonic:** HIGHAMTCHK
- **Parameter Values:** 20000;Amazon

This sample rule performs the following:

1. Parses the extensible element string ("amount=70000;merchant=Amazon") that is passed in the **evaluateRisk()** API call by the tag "amount" and extracts the value of amount in a variable, say ActualAmount.
2. Extracts the parameter value (20000) for the rule, and stores it in a variable, say ParameterAmount.
3. Because ActualAmount (70000), in this case, is greater than ParameterAmount (20000), the Add-On rule returns "Matched".

Similar to the preceding example, the capability to monitor other aspects of banking transactions (such as, Cumulative Amount Velocity Check) can also be implemented as an Add-On rules.

**NOTE:** Based on your business requirements, you can select and deploy any number of Add-On rules.

Unlike the pre-defined out-of-box rules, Add-On rules are not deployed automatically when you install RiskFort. You must use the **Add-On Rules Configuration** page (Figure 3-19) to specify the additional rules that you want to deploy.

**Figure 3-19**

Welcome Admin | Global | Global Admin  
Last Login Time

User Profile | Logout

### Add-On Rules Configuration

Deploy a new Add-On Rule. You can also update or remove an existing Add-On Rule.

Note: The changes on this screen will be effective only if you:

1. Enable the rule on the Scoring Configuration page.
2. Migrate to Production.
3. Refresh the RiskFort Server Cache.

Select Deployed Rule or Add New:

Rule Name:

Description:

Library Name:

This file must be present in the RiskFort Server machine in the location for Add-On Rule libraries.

Rule Mnemonic:   
(Max. 25 characters) This will be used in logging, in APIs etc.

Parameters (Name=Value):

**IMPORTANT:** If this rule needs more than one parameter, then it is recommended that you enter name=parameter values separated with a delimiter (For example, a semicolon) so that the add on rule can parse the data.

Use the Add-On Rules Configuration page for:

- [Deploying an Add-On Rule](#)
- [Editing the Attributes of a Deployed Add-On Rule](#)
- [Removing a Deployed Add-On Rule](#)

### Deploying an Add-On Rule

To deploy an Add-On rule, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Add-On Rules**.

The Add-On Rules Configuration page appears, as shown in [Figure 3-19](#).

2. From the **Select Deployed Rule or Add New** list, select the **Add New Rule** option.
3. Specify the name of the rule in the **Rule Name** field.

**NOTE:** This name will appear in the Scoring Configuration screen.

4. Enter useful information related to the Add-On rule for later reference in the **Description** field.
5. Specify the file name (*without* the extension) of the library for the Add-On rule in the **Library File** field.

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

- **Windows:** `<install_location>\Arcot Systems\plugins\rules\addon\`
- **UNIX-based platforms:**  
`<install_location>/arcot/plugins/rules/addon/`

6. Specify a short name for the rule in the **Rule Mnemonic** field.

The maximum length of the Mnemonic is 15 characters and no spaces are allowed.

**NOTE:** This mnemonic is used for logging purposes and in APIs.

7. Enter the default value(s) that the rule must check against for each transaction in real time in the **Parameter Values** field.

If the rule defines more than one parameters, then you *must*:

- Enter these values in the same sequence as defined in the rule.

For example, in [Add-On Rule Example](#) discussed on [page 63](#), you must specify the values as **20000;Amazon**. If you change the sequence of these parameter values (for example, Amazon;20000), then the rule might not work as intended.

- Delimit successive values with ; (semicolon).
8. Click **Save** to deploy the rule.
  9. 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.

10. To make the changes active, you must migrate them to production.  
Refer to [“Migrating to Production”](#) for instructions to do so.
11. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
  - a. Navigate to the following directory:

#### On Windows:

```
<install_location>\Arcot Systems\bin\
```

#### On UNIX Platforms:

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

### Editing the Attributes of a Deployed Add-On Rule

To edit the attributes of a deployed Add-On rule, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Add-On Rules**.  
The Add-On Rules Configuration page appears, as shown in [Figure 3-19](#).
2. From the **Select Deployed Rule or Add New** list, select the name of the rule you want to modify.
3. Make the required changes.
4. Click **Save** to save the changes to the rule.
5. Ensure that the rule is enabled. Refer to [“Configuring Scoring”](#) for instructions to do so.

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](#)” for instructions to do so.
7. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
  - a. Navigate to the following directory:

**On Windows:**

```
<install_location>\Arcot Systems\bin\
```

**On UNIX  
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

**Removing a Deployed Add-On Rule**

To remove a deployed Add-On rule, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Add-On Rules**.  
The Add-On Rules Configuration page appears, as shown in [Figure 3-19](#).
2. From the **Select Deployed Rule or Add New** list, select the name of the rule you want to remove.
3. Click **delete** to remove the rule.  
The changes are yet not active, and not available to your end users.
4. To make the changes active, you must migrate them to production.  
Refer to “[Migrating to Production](#)” for instructions to do so.
5. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:
  - a. Navigate to the following directory:

**On Windows:**

```
<install_location>\Arcot Systems\bin\
```

**On UNIX  
Platforms:**

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

# Configuring Callouts

**NOTE:** Implementation of Callouts is optional.

Based on your business requirements, you can also write your own custom Evaluation rule and Scoring logic that, 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-1.7-sample-callouts.war`) that demonstrates how you can write and implement simple Evaluation and Scoring Callouts. See [Appendix A, “Working with Sample Callouts”](#) 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 Scoring Configuration page ([Figure 3-18](#)) for it to take effect.

## Callout Implementation

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.

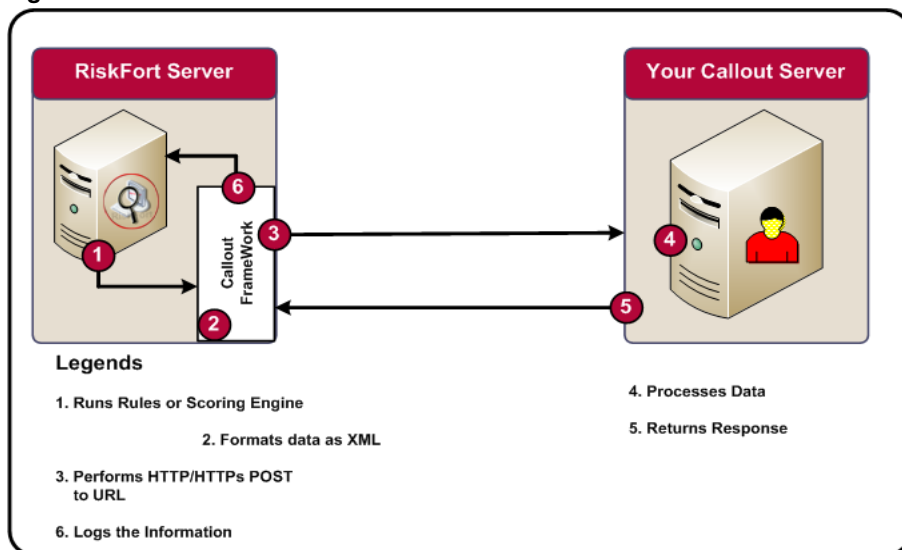
If the response is not received within the specified time-out period, then the framework returns `FAILURE` as rule result and empty strings ( " " ) for the modifier and annotation.

**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.

The following figure illustrates the interaction between RiskFort Server, Callout Framework, and your Callout.

Figure 3-20



**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.

### Evaluation Callouts

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.
  - **Extensible elements**, 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 Callouts

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.
  - **Extensible elements**, 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.

Use the Callout Configuration page, as shown in the following figure (**Figure 3-21**) for:

- **Configuring Evaluation Callouts**
- **Configuring Scoring Callouts**

Figure 3-21



**ARCOT**

Welcome Admin Global | Global Admin  
Last Login Time 11/13/2008 07:44:15 AM GMT  
[User Profile](#) | [Logout](#)

---

**Admin Configurations**

**WebFort Configurations**

**Issuance Configurations**

**SignFort Configurations**

**RiskFort Configurations**

- Trusted IP/Aggregator Setup
- Negative IP Types
- Negative IP Address
- Protocol Setup
- Update Negative Country List
- Velocity Check
- Zone Hopping Check
- Add-On Rules
- Callout Configuration
- Scoring Configuration
- System Configuration
- Migrate to Production

**Reports**

### Callout Configuration

Configure Evaluation and Scoring Callouts.

*Note: The changes on this screen affect the staging (proposed) data only. To make these changes active (in production), the following need to be done:*

1. Migrate to Production
2. Refresh the RiskFort Server Cache

---

#### Evaluation Callout Configuration

| Callout Elements                                                   | Active                                                                                                                                                                           | Proposed                                                                                                                                                                                                                     |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Authentication SSL:                                         | YES                                                                                                                                                                              | <input checked="" type="radio"/> YES <input type="radio"/> NO                                                                                                                                                                |
| Client Authentication SSL:                                         | NO                                                                                                                                                                               | <input type="radio"/> YES <input checked="" type="radio"/> NO                                                                                                                                                                |
| URL of Callout:                                                    | https://kiran                                                                                                                                                                    | <input type="text" value="https://eval"/>                                                                                                                                                                                    |
| Connection Timeout: (Seconds)                                      | 30                                                                                                                                                                               | <input type="text" value="30"/>                                                                                                                                                                                              |
| Receive Timeout: (Seconds)                                         | 11                                                                                                                                                                               | <input type="text" value="11"/>                                                                                                                                                                                              |
| Callout Server Root Certificate:                                   | Issuer: EMAILADDRESS=kiran@arcot.com, CN=kiranCA, OU=Admin, O=Arcot Systems, L=Bangalore, ST=Karnataka, C=IN<br>Valid From: 09/12/2008 01:12:49<br>Valid To: 10/12/2008 01:12:49 | Issuer: EMAILADDRESS=kiran@arcot.com, CN=kiranCA, OU=Admin, O=Arcot Systems, L=Bangalore, ST=Karnataka, C=IN<br>Valid From: 09/12/2008 01:12:49<br>Valid To: 10/12/2008 01:12:49<br><input type="button" value="Browse..."/> |
| RiskFort Server Certificate and Private Key: (For Client Auth SSL) | N/A                                                                                                                                                                              | Certificate: <input type="button" value="Browse..."/><br>Private Key: <input type="button" value="Browse..."/>                                                                                                               |
| Callout Description:                                               | Evaluation Callout for safebank                                                                                                                                                  | <input type="text" value="Evaluation Callout for safebank"/>                                                                                                                                                                 |

---

#### Scoring Callout Configuration

| Callout Elements                                                   | Active                       | Proposed                                                                                                       |
|--------------------------------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------|
| Server Authentication SSL:                                         | NO                           | <input type="radio"/> YES <input checked="" type="radio"/> NO                                                  |
| Client Authentication SSL:                                         | NO                           | <input type="radio"/> YES <input checked="" type="radio"/> NO                                                  |
| URL of Callout:                                                    | http://scoring               | <input type="text" value="http://scoring"/>                                                                    |
| Connection Timeout: (Seconds)                                      | 40                           | <input type="text" value="40"/>                                                                                |
| Receive Timeout: (Seconds)                                         | 33                           | <input type="text" value="33"/>                                                                                |
| Callout Server Root Certificate:                                   | N/A                          | <input type="button" value="Browse..."/>                                                                       |
| RiskFort Server Certificate and Private Key: (For Client Auth SSL) | N/A                          | Certificate: <input type="button" value="Browse..."/><br>Private Key: <input type="button" value="Browse..."/> |
| Callout Description:                                               | Scoring callout for safebank | <input type="text" value="Scoring callout for safebank"/>                                                      |

**NOTE:** RiskFort is shipped with a basic Sample Callouts WAR file (riskfort-1.7-sample-callouts.war) that demonstrates how you can write and implement Evaluation and Scoring Callouts. See [Appendix A, “Working with Sample Callouts”](#) for more information on deploying and configuring this file.

## Configuring Evaluation Callouts

To configure an Evaluation Callout, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Callout Configuration**.

The Callout Configuration page appears, as shown in [Figure 3-21](#).

2. In the **Evaluation Callout Configuration** 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 of (your) Callout**:

- 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 **Receive Timeout** in seconds.

*Receive 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 *or* **Client Authentication SSL** is set to YES, then you *must* specify the **Callout Server Root Certificate**.
- **Callout Server Root Certificate** *must* 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 *must* specify the **Callout Server Root Certificate** and **RiskFort Server Certificate and Private Key**.
- **RiskFort Server Certificate and Private Key** *must* be in .PEM (Base64-encoded) format.

- h. Specify useful details about the Callout against **Callout Description**.

3. Click **Save** to save the changes that you just made.

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

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

Refer to “[Migrating to Production](#)” for instructions to do so.

5. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:

- a. Navigate to the following directory:

#### On Windows:

```
<install_location>\Arcot Systems\bin\
```

#### On UNIX Platforms:

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

## Configuring Scoring Callouts

To configure a Scoring Callout, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Callout Configuration**.

The Callout Configuration page appears, as shown in [Figure 3-21](#).

2. In the **Scoring Callout Configuration** 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 of (your) Callout**:

- 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 **Receive Timeout** in seconds.

*Receive 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 *or* **Client Authentication SSL** is set to YES, then you *must* specify the **Callout Server Root Certificate**.
- **Callout Server Root Certificate** *must* 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 *must* specify the **Callout Server Root Certificate** and **RiskFort Server Certificate and Private Key**.
- **RiskFort Server Certificate and Private Key** *must* be in .PEM (Base64-encoded) format.

- h. Specify useful details about the Callout against **Callout Description**.

3. Click **Save** to save the changes that you just made.

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

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

Refer to “[Migrating to Production](#)” for instructions to do so.

5. Run the **aradmin** tool to refresh the RiskFort Server cache as follows:

- a. Navigate to the following directory:

#### On Windows:

```
<install_location>\Arcot Systems\bin\
```

#### On UNIX Platforms:

```
<install_location>/arcot/bin/
```

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

# Migrating to Production

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

- Trusted IPs and Aggregators
- Negative IP Address List
- Negative Country List
- User Velocity Check
- Device Velocity Check
- Zone Hopping Check
- Add-On Rules
- Callouts
- Scoring

When the data related to the preceding list is being configured, it is referred to as *Staging data*. This data can be created over a period of time by using several administrative sessions. While you configure this data, it is stored in the *Staging data area* and the **Proposed** column on respective configuration page reflects this data. Similarly, any changes that you make to the Proposed column affect the Staging data. As a result, the terms "proposed" and "Staging data" are equivalent and are used interchangeably in this guide.

When all data is configured according to your requirements, then the Staging 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 [aradmin \(RiskFort Server Refresh and Shutdown Tool\)](#) tool. At any point of time, RiskFort Servers work with Active data configurations only.

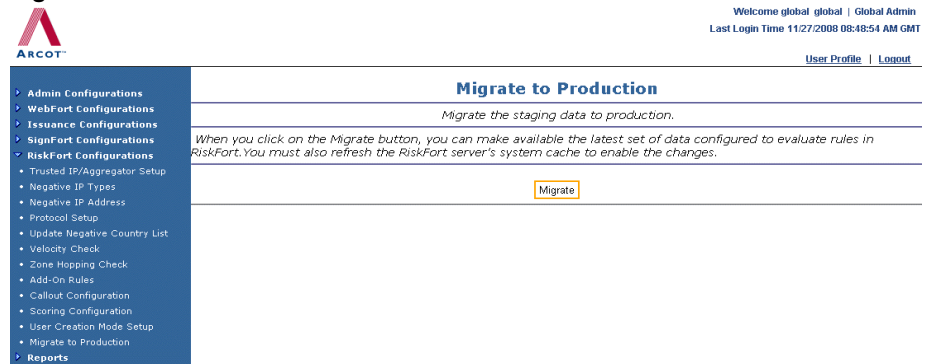
After the Staging data is migrated to Active data, the Staging data area becomes empty. Subsequently for any attempts to configure RiskFort data, a copy of the Active data is created in Staging data area. Further additions or deletions can be done to the Staging data until configurations are ready for migrating to production. All modifications are reflected only in the Staging data. However, Reports are available to view Active or Staging configurations.

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

When changes are made to existing configurations, the changes are confined to the Staging area *only*. To commit these changes for RiskFort Server to be able to use them (in other words, update the new configurations to Active area), you *must* migrate the data to production.

The following figure shows the Migrate to Production page that you can use to do so.

**Figure 3-22**



To migrate to production, perform the following steps:

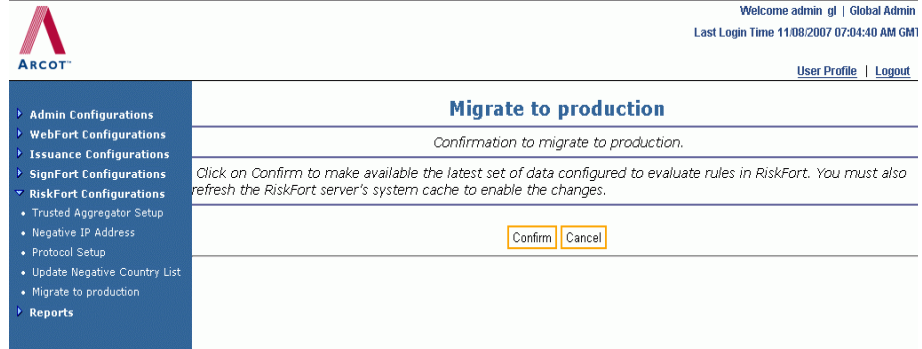
1. Under **RiskFort Configurations** on the side-bar menu, select **Migrate to Production**.

The Migrate to Production page is displayed, as shown in [Figure 3-22](#).

2. Click **Migrate**.

The page to confirm the action is displayed, as shown in the following figure.

Figure 3-23



3. On the confirmation page, click **Confirm** to start the migration process.

The "Migrated to production successfully." message is displayed.

**NOTE:** Ensure that you refresh the server cache after you complete the migration. Your changes will become active only after you do so.

## Chapter 4

# Working with RiskFort Reports

RiskFort Reports provide details of risk-evaluation transactions performed by the RiskFort Server. These reports also record day-to-day operations performed by the administrators.

In a RiskFort-based system, administrators can generate the following types of reports:

- **Administrator Activity Reports**
- **RiskFort Configuration Data Reports**
- **RiskFort Transaction Reports**

**NOTE:** The activity timings displayed in all Reports are in server time zone.

Section “**Exporting Reports to a File**” in this chapter discusses how to export generated reports to a file.

# Administrator Activity Reports

This section explains the reports that provide detailed information related to all activities performed by RiskFort administrators. The activity reports that belong to this category are:

- [Administrator Activity Audit Reports](#)
- [Authentication Activity Report](#)

## Administrator Activity Audit Reports

This report lists all activities of all administrators using the Administration Console. An administrator can view this report only if they have privileges for the ADMINISTRATORS group. As a result, this report can be generated by Master Administrator and Global Administrators.

The following figure displays the Administrator Activity Audit Report page.

**Figure 4-1**

| Administrator Activity Audit Report                                                                                         |             |             |                            |                                   |                |             |         |          |                 |             |                |
|-----------------------------------------------------------------------------------------------------------------------------|-------------|-------------|----------------------------|-----------------------------------|----------------|-------------|---------|----------|-----------------|-------------|----------------|
| This report displays activity taken by administrators in the Arcot Admin Console.                                           |             |             |                            |                                   |                |             |         |          |                 |             |                |
| <div>Export</div> <div>New Report</div>                                                                                     |             |             |                            |                                   |                |             |         |          |                 |             |                |
| User name used for search is : Alan Date Range: From: 08/23/2006 Through: 08/23/2007<br>1 2 3 4 5 6 7 8 9 10 11 12 (Next >) |             |             |                            |                                   |                |             |         |          |                 |             |                |
| Date                                                                                                                        | User Name   | Resource    | Event Type                 | Session Id                        | Target Group   | Target User | Status  | Event Id | Caller Id       | Instance Id | Admin Group    |
| 08/22/2007 12:21:07                                                                                                         | ALANJOHNSON | LOGOUT      | LOGOUT                     | 472DFF1F7C88A5B8416827AFE96862F8  | N/A            | N/A         | Success | 38020    | ARCOT_WEB_ADMIN | 1           | ADMINISTRATORS |
| 08/22/2007 12:21:00                                                                                                         | ALANJOHNSON | AUTH_CONFIG | DISABLE_CREDENTIAL         | 472DFF1F7C88A5B8416827AFE96862F8  | ADMINISTRATORS | MARIAJAMES  | Success | 38019    | ARCOT_WEB_ADMIN | 1           | ADMINISTRATORS |
| 08/22/2007 12:20:37                                                                                                         | ALANJOHNSON | LOGIN       | LOGIN                      | 472DFF1F7C88A5B8416827AFE96862F8  | N/A            | N/A         | Success | 38018    | ARCOT_WEB_ADMIN | 1           | ADMINISTRATORS |
| 08/21/2007 14:59:52                                                                                                         | ALANJOHNSON | LOGIN       | LOGIN                      | 398C7EEACF1869A765E971EDAE408CD80 | N/A            | N/A         | Success | 33006    | ARCOT_WEB_ADMIN | 1           | ADMINISTRATORS |
| 08/21/2007 10:04:59                                                                                                         | ALANJOHNSON | LOGIN       | LOGIN                      | 9E4487751DBFAE94FB9BA066F8A4900   | N/A            | N/A         | Success | 26029    | ARCOT_WEB_ADMIN | 1           | ADMINISTRATORS |
| 08/20/2007 19:54:19                                                                                                         | ALANJOHNSON | REPORT      | VIEW_ADMIN_AUDITLOG_REPORT | 519F882CE5346107DCB7E586B92AF02B  | N/A            | N/A         | Success | 26028    | N/A             | 1           | ADMINISTRATORS |

The following table lists the information included in an Administrator Activity Audit Report:

**Table 4-1** Administrator Activity Audit Report Fields

| Report Field | Description                                               |
|--------------|-----------------------------------------------------------|
| Date         | The date and time of the activity.                        |
| User Name    | The name of the administrator who performed the activity. |

**Table 4-1** Administrator Activity Audit Report Fields

| Report Field | Description                                                                                                                                                                                         |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource     | The resource created, modified, deleted, read, or viewed by the administrator.                                                                                                                      |
| Event Type   | The type of activity (such as create, read, modify, delete, or view) that is performed by the administrator.                                                                                        |
| Session Id   | The identifier of the application server session to which the Administrator has logged in.                                                                                                          |
| Target Group | The group to which the Target User belongs.                                                                                                                                                         |
| Target User  | The name of the user whose attributes were administered by the administrator.                                                                                                                       |
| Status       | The status of the action taken. Action status can be:<br><br><b>Success</b> - If the action was completed successfully.<br><br><b>Failure</b> - If the administrator failed to complete the action. |
| Event Id     | The unique ID for every activity performed by the administrator.                                                                                                                                    |
| Caller Id    | The unique identifier set by the calling application. Caller ID can be blank, if the calling application does not set the value.                                                                    |
| Instance Id  | The unique identifier to identify the server instance.                                                                                                                                              |
| Admin Group  | The group to which the administrator belongs.                                                                                                                                                       |

To generate an Administrator Activity Audit Report, perform the following tasks:

1. Under **Reports** menu on the left-hand, click **Administrator Activity Audit Report**.

The Administrator Activity Audit Report page is displayed, as shown in the following figure.

Figure 4-2

The screenshot shows the 'Administrator Activity Audit Report' page. On the left is a blue sidebar with a navigation menu. The top right of the page displays user information: 'Welcome admin | Global Adm' and 'Last Login Time 11/08/2007 07:04:40 AM C'. Below this is a 'User Profile | Logout' link. The main content area has a title 'Administrator Activity Audit Report' and a subtitle 'Select administrator activity to display.'. Below the subtitle are search filters: 'Date Range:' with a 'Custom' dropdown, 'From:' with a date field '11/08/2007', and 'Through:' with a date field '11/08/2007'. There is also a 'Group' dropdown set to 'ADMINISTRATORS' and a 'User Name' text field. At the bottom of the filters are 'Clear' and 'Display Report' buttons.

**ARCOT™**

Welcome admin | Global Adm  
Last Login Time 11/08/2007 07:04:40 AM C

User Profile | Logout

### Administrator Activity Audit Report

Select administrator activity to display.

Date Range: Custom From: 11/08/2007 Through: 11/08/2007

Group: ADMINISTRATORS User Name

Clear Display Report

**Admin Configurations**

**WebFort Configurations**

**Issuance Configurations**

**SignFort Configurations**

**RiskFort Configurations**

**Reports**

- Administrator Activity Audit Report
- Credential Management Report
- Authentication Activity Report
- Signing Activity Report
- Digital ID Management Report
- RiskFort Trusted Aggregator Report
- RiskFort Negative IP Report
- RiskFort Exception User Report
- Risk Advice Summary Report
- RiskFort Negative Country Report
- Risk Evaluation Detail Activity Report

2. Select the **Date Range** from the drop-down menu.

You can also select a pre-defined date range in the **From** and **Through** fields.

3. If required, enter the name of an administrator in the **User Name** field for further filtering the data.
4. Select one of the following groups from the **Group** drop-down menu:
  - **ADMINISTRATORS**: Refers to administrators' group.
  - **GROUP2**: Refers to users of the group.

**NOTE:** The Group drop-down menu appears only if the administrator performing this activity has privileges for more than one group.

5. Click **Display Report** to view the generated report.
6. Click **Export** to save the report to a file.

For more information on how to export reports, refer to the section “[Exporting Reports to a File.](#)”

# Authentication Activity Report

This report provides details of activities that were performed by users authenticating with RiskFort.

The following figure shows a sample Authentication Activity Report.

**Figure 4-3**

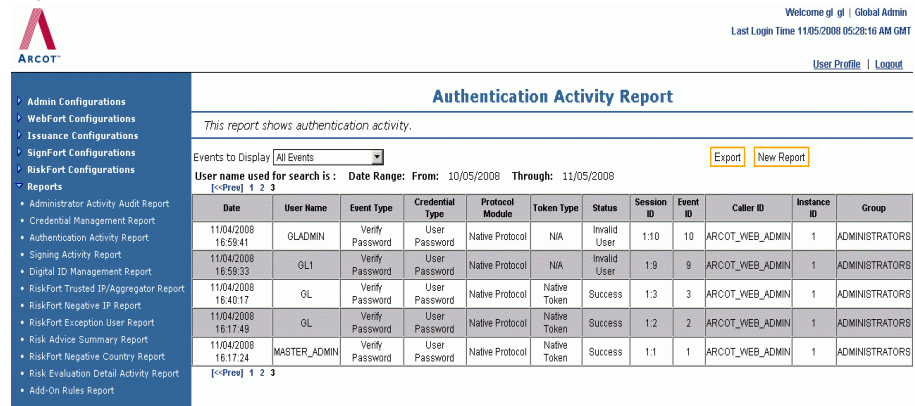


Table 4-2 describes the information included in the Authentication Activity Report.

**Table 4-2** Authentication Activity Report Fields

| Report Field    | Description                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Date            | The date and time of login.                                                                                                                                                                                                                      |
| User Name       | The name of the user who has authenticated with the WebFort server.                                                                                                                                                                              |
| Event Type      | The type of event that took place for the activity.                                                                                                                                                                                              |
| Credential Type | The type of the credential issued to the user.                                                                                                                                                                                                   |
| Protocol Module | The protocol used for authentication.                                                                                                                                                                                                            |
| Token Type      | The token issued to the user after successful authentication. The token type typically is <b>Native</b> , which is an Arcot proprietary token. The token can be used multiple times for verification during the configured validity period.      |
| Status          | The status of the action taken. Action status can be: <ul style="list-style-type: none"> <li><b>Success</b> - If the action was completed successfully.</li> <li><b>Failure</b> - If the administrator failed to complete the action.</li> </ul> |
| Session ID      | The session ID for the transaction provided by the Web server.                                                                                                                                                                                   |

**Table 4-2** Authentication Activity Report Fields

| Report Field | Description                                                                                                                     |
|--------------|---------------------------------------------------------------------------------------------------------------------------------|
| Event ID     | The generated event ID.                                                                                                         |
| Caller ID    | The unique identifier set by the calling application. Caller Id can be blank if the calling application does not set the value. |
| Instance ID  | The ID to identify the server instance.                                                                                         |
| Group        | The group to which the specified administrator belongs.                                                                         |

**To generate an Authentication Activity Report:**

1. In the left pane, under **Reports** menu, click the **Authentication Activity Report** link.  
  
The Authentication Activity Report page appears.
2. Select the **Date Range** from the drop-down list or enter a predefined date range in the **From** and **Through** fields
3. Enter the **User Name** of the user whose authentication activity details has to be displayed.
4. Select the **Group** from the drop-down list.
5. Click the **Display Report** button to view the report generated for the administrator.
6. Select an event, if required, from the **Events to Display** drop-down list.
7. Click the **Export** button to save the file. Refer to the section [“Exporting Reports to a File”](#) for more information on exporting the report.

Click the **New Report** button to make a new selection.

# RiskFort Configuration Data Reports

This section explains the configuration data reports available to RiskFort administrators. The data reports that belong to this category are:

- [RiskFort Trusted IP/Aggregator Report](#)
- [RiskFort Negative IP Report](#)
- [RiskFort Negative Country Report](#)
- [RiskFort Exception User Report](#)
- [RiskFort Add-On Rules Report](#)

## RiskFort Trusted IP/Aggregator Report

This report provides the list of trusted aggregators configured in the system and their Internet Protocol (IP) address ranges. This report is available for both staging as well as active data. (See “[Configuring Trusted Aggregators](#)” on page 38 for more information on Trusted Aggregators.)

The Trusted IP/Aggregator Report page that displays information related to Trusted IP is shown in the following figure.

**Figure 4-4**

| RiskFort Trusted IP/Aggregator Report                                |                |                            |                     |
|----------------------------------------------------------------------|----------------|----------------------------|---------------------|
| <i>This report provides the list of trusted IPs and Aggregators.</i> |                |                            |                     |
|                                                                      |                | Staging Data ▾ TRUSTEDIP ▾ | Show Export         |
| IP Address                                                           | End IP Address | Mask                       | Date Created        |
| 74.120.68.40                                                         | 74.132.80.80   | N/A                        | 01/12/2009 18:41:02 |

The following table lists the information included in a RiskFort Trusted IP Report:

**Table 4-3** Trusted Aggregator Report Fields

| Field          | Description                                                 |
|----------------|-------------------------------------------------------------|
| 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. |

**Table 4-3** Trusted Aggregator Report Fields

| Field        | Description                                               |
|--------------|-----------------------------------------------------------|
| Date Created | The date when the first aggregator device ID was created. |

The Trusted IP/Aggregator Report page that displays information related to Trusted Aggregator is shown in the following figure.

**Figure 4-5**

| RiskFort Trusted IP/Aggregator Report                                                               |              |                |               |                                                                  |                     |                        |              |                        |              |                        |
|-----------------------------------------------------------------------------------------------------|--------------|----------------|---------------|------------------------------------------------------------------|---------------------|------------------------|--------------|------------------------|--------------|------------------------|
| This report provides the list of trusted IPs and Aggregators.                                       |              |                |               |                                                                  |                     |                        |              |                        |              |                        |
| <div> <div>Staging Data</div> <div>TRUSTEDAGGREGATOR</div> <div>Show</div> <div>Export</div> </div> |              |                |               |                                                                  |                     |                        |              |                        |              |                        |
| Aggregator Name                                                                                     | IP Address   | End IP Address | Mask          | Aggregator Device ID 1                                           | Date Created        | Aggregator Device ID 2 | Date Created | Aggregator Device ID 3 | Date Created | Aggregator Device ID 4 |
| k3k                                                                                                 | 64.193.82.28 | N/A            | 255.255.252.0 | lubhkp+z+E3PybX6iil+ouU9JBf9XfZ9IXhQvJZoAMyOBrngtalq9fBtuJkOaQ55 | 01/12/2009 18:44:43 | N/A                    | N/A          | N/A                    | N/A          | N/A                    |

The following table lists the information included in a RiskFort Trusted Aggregator Report:

**Table 4-4** Trusted Aggregator Report Fields

| Field                 | Description                                                 |
|-----------------------|-------------------------------------------------------------|
| Aggregator Name       | The name of the aggregator.                                 |
| 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. |
| Aggregator Device ID1 | The unique device ID of the trusted aggregator.             |
| Date Created          | The date when the first aggregator device ID was created.   |
| Aggregator Device ID2 | The second device ID generated for the aggregator.          |
| Date Created          | The date when the second aggregator device ID was created.  |
| Aggregator Device ID3 | The third device ID generated for the aggregator.           |
| Date Created          | The date when the third aggregator device ID was created.   |

To generate a Trusted IP/Aggregator Report, perform the following steps:

1. Under **Reports** menu on the left-hand, click **RiskFort Trusted IP/Aggregator Report**.

The RiskFort Trusted Aggregator Report page is displayed.

- From the drop-down menu of the report, select **Active Data** or **Staging Data**.

For more information on Active and Staging data, refer to the section, “[Migrating to Production.](#)”

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

- Trusted IP**, to display the report for all Trusted IP addresses registered in the system.
- Trusted Aggregator**, to display the report for all Trusted Aggregators registered in the system.

- Click **Show** to display the selected report type.

- Click **Export** to save the report to a file.

For more information on how to export reports, refer to the section, “[Exporting Reports to a File.](#)”

## RiskFort Negative IP Report

This report shows the list of negative IP address ranges configured in the system. This report is available for both staging as well as active data. (See “[Configuring Negative IP Address List](#)” on page 49 for more information on Negative IP List.)

The following figure displays the RiskFort Negative IP Report page.

**Figure 4-6**

| RiskFort Negative IP Report                                     |                |               |                                           |
|-----------------------------------------------------------------|----------------|---------------|-------------------------------------------|
| This report provides the list of currently untrusted IP ranges. |                |               |                                           |
|                                                                 |                |               | <div>Staging Data</div> <div>Export</div> |
| IP Address                                                      | End IP Address | Mask          | Source                                    |
| 12.12.1.12                                                      | N/A            | 33.33.33.33   | Pakistan                                  |
| 125.17.166.160                                                  | N/A            | 255.255.252.0 | N/A                                       |

The following table lists the information included in the Negative IP List Report.

**Table 4-5** Negative IP Report Fields

| Fields         | Description                                             |
|----------------|---------------------------------------------------------|
| 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. |

**Table 4-5** Negative IP Report Fields

| Fields | Description                                    |
|--------|------------------------------------------------|
| Source | The vendor who supplied the negative IP range. |
| Type   | Type of negative IP address.                   |

To generate a Negative IP Report, perform the following steps:

1. Under **Reports** menu on the left-hand, click **RiskFort Negative IP Report**.  
The RiskFort Negative IP Report page is displayed.
2. From the drop-down menu above the report, select **Active Data** or **Staging Data**.  
For more information on Active and Staging data, refer to the section, [“Migrating to Production.”](#)
3. Click **Export** to save the report to a file. For more information on how to export reports, refer to the section, [“Exporting Reports to a File.”](#)

## RiskFort Negative Country Report

This report shows the list of negative countries configured in the system. This report is available for both staging and active data. (See [“Configuring Velocity Check” on page 51](#) for more information on Negative Country List.)

The following figure displays the Negative Country Report page.

**Figure 4-7**

| RiskFort Negative Country Report                                    |                                        |                                                    |
|---------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
| <i>This report provides the current list of negative countries.</i> |                                        |                                                    |
|                                                                     |                                        | Staging Data <input type="button" value="Export"/> |
| ISO Country Code                                                    | Country                                | Date Created                                       |
| AF                                                                  | AFGHANISTAN                            | 08/09/2007 12:43:40                                |
| IR                                                                  | IRAN, ISLAMIC REPUBLIC OF              | 08/09/2007 12:43:40                                |
| KP                                                                  | KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF | 08/09/2007 12:43:40                                |
| NG                                                                  | NIGERIA                                | 08/09/2007 12:43:40                                |

The following table lists the information included in a Negative Country Report.

**Table 4-6** Negative Country Report Fields

| Fields           | Description                                  |
|------------------|----------------------------------------------|
| ISO Country Code | The code assigned to every country by ISO.   |
| Country          | The name of the country.                     |
| Date Created     | Date when the country was added to the list. |

To generate a Negative Country Report, perform the following steps:

1. Under **Reports** menu on the left-hand, click **RiskFort Negative Country Report**.

The RiskFort Negative Country Report page is displayed.

2. From the drop-down menu above the report, select **Active Data** or **Staging Data**.

For more information on Active and Staging data, refer to the section, “[Migrating to Production](#).”

3. Click **Export** to save the report to a file.

For more information on how to export reports, refer to the section, “[Exporting Reports to a File](#).”

## RiskFort Exception User Report

This report shows the list of Exception users in the RiskFort system. The following figure displays the RiskFort Exception User Report page.

**Figure 4-8**

| RiskFort Exception User Report                                                                        |                     |          |          |            |
|-------------------------------------------------------------------------------------------------------|---------------------|----------|----------|------------|
| <i>This report shows the time period and reason settings for specific exception users.</i>            |                     |          |          |            |
| <div> <div>Date Range: From: 08/09/2007 Through: 08/09/2007</div> <div>Export New Report</div> </div> |                     |          |          |            |
| Date Start                                                                                            | Date End            | Username | Reason   | Group Name |
| 08/09/2007 00:00:00                                                                                   | 08/08/2007 23:50:40 | JCHOI    | VIP User | Group 2    |

The following table lists the information included in a RiskFort Exception Users Report:

**Table 4-7** RiskFort Exception Users Report Fields

| Fields     | Description                                                                          |
|------------|--------------------------------------------------------------------------------------|
| Date Start | The date and time from which the user is considered an exception user in the system. |
| Date End   | The date and time when the user stops being an exception user in the system.         |
| Username   | The unique user name.                                                                |
| Reason     | The reason for making the user an Exception User in the system.                      |
| Group Name | The group to which the administrator belong.                                         |

To generate RiskFort Exception User Report, perform the following steps:

1. Under **Reports** menu on the left-hand, click **RiskFort Exception User Report**.  
The RiskFort Exception User Report page is displayed.
2. Select the **Date Range** from the drop-down menu.  
You can also select a pre-defined date range in the **From** and **Through** fields.
3. If required, enter the name of an administrator in the **User Name** field for further filtering the data.
4. Select one of the following groups from the **Group** drop-down menu:
  - **ADMINISTRATORS**: Refers to administrators' group.
  - **GROUP2**: Refers to users of the group.

**NOTE:** The Group drop-down menu appears only if the administrator performing this activity has privileges for more than one group.
5. Click **Display Report** to view the generated report.
6. Click **Export** to save the report to a file.

For more information on how to export reports, refer to the section [“Exporting Reports to a File.”](#)

## RiskFort Add-On Rules Report

RiskFort Add-On Rules Report provides an overall summary of Add-On rules that are configured in the system. (See “[Configuring Add-On Rules](#)” on page 63 for detailed information on Add-On rules.)

The following figure displays a Add-On Rules Report page.

**Figure 4-9**

| Add-On Rules Report                                     |         |                |                    |            |                                                                                |
|---------------------------------------------------------|---------|----------------|--------------------|------------|--------------------------------------------------------------------------------|
| This report provides the list of deployed Add-On Rules. |         |                |                    |            |                                                                                |
|                                                         |         |                |                    |            | Active Data <input type="button" value="Export"/>                              |
| Rule Name                                               | Enabled | Mnemonic       | Library Name       | Parameters | Description                                                                    |
| High Amount Check                                       | 0       | HIGHAMTCHECK   | highamtcheck.dll   | 500000     | To put a limit on the amount of transaction.                                   |
| Max Session Check                                       | 0       | MAXSESSION     | maxsession.dll     | 3          | To put a limit on no.of sessions being active simultaneously for a single user |
| Behaviour Check                                         | 0       | BEHAVIUORCHECK | behaviuorcheck.dll | N/A        | Adaptive Risk Scoring engine depending the user behaviour analysis.            |

The following table lists the information included in an Add-On Rules Report:

**Table 4-8** Add-On Rules Report Fields

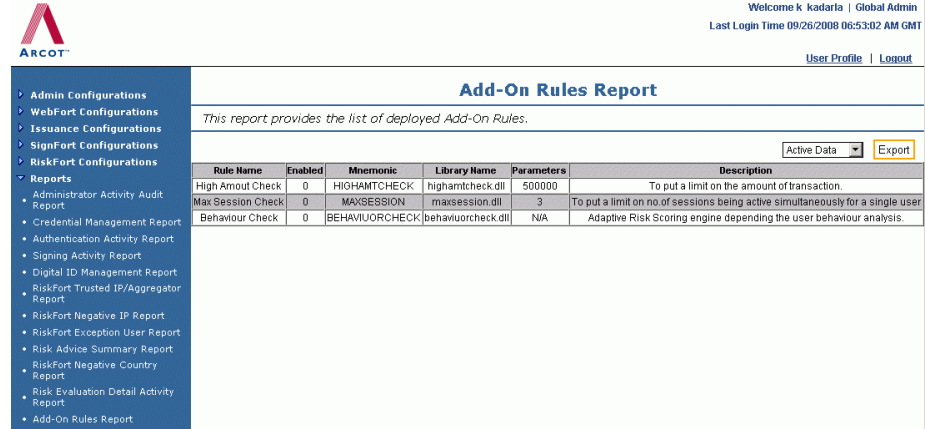
| Fields       | Description                                                                         |
|--------------|-------------------------------------------------------------------------------------|
| Rule Name    | The name of the Add-On rule.                                                        |
| Enabled      | The indication whether the rule is being used or not at the time the report is run. |
| Mnemonic     | The short name of the Add-On rule.                                                  |
| Library Name | The name of the .dll or .so file associated with the rule.                          |
| 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.                 |

To generate an Risk Advice Summary Report, perform the following tasks:

1. Under **Reports** menu on the left-hand, click **RiskFort Add-On Rules Report**.

The Add-On Rules Report page is displayed, as shown in the following figure.

Figure 4-10



Welcome k katarla | Global Admin  
Last Login Time 09/26/2008 06:53:02 AM GMT  
[User Profile](#) | [Logout](#)

### Add-On Rules Report

*This report provides the list of deployed Add-On Rules.*

Active Data [Export](#)

| Rule Name         | Enabled | Mnemonic       | Library Name       | Parameters | Description                                                                     |
|-------------------|---------|----------------|--------------------|------------|---------------------------------------------------------------------------------|
| High Amount Check | 0       | HIGHAMTCHECK   | highamtcheck.dll   | 500000     | To put a limit on the amount of transaction.                                    |
| Max Session Check | 0       | MAXSESSION     | maxsession.dll     | 3          | To put a limit on no. of sessions being active simultaneously for a single user |
| Behaviour Check   | 0       | BEHAVIUORCHECK | behaviuorcheck.dll | N/A        | Adaptive Risk Scoring engine depending the user behaviour analysis.             |

- From the drop-down menu above the report, select **Active Data** or **Staging Data**.

For more information on Active and Staging data, refer to the section, “[Migrating to Production.](#)”

- Click **Export** to save the report to a file.

For more information on how to export reports, refer to the section, “[Exporting Reports to a File.](#)”

# RiskFort Transaction Reports

This section explains the transaction reports that are available to RiskFort administrators. The transaction reports that can be generated under this category are:

- [Risk Advice Summary Report](#)
- [Risk Evaluation Detail Activity Report](#)

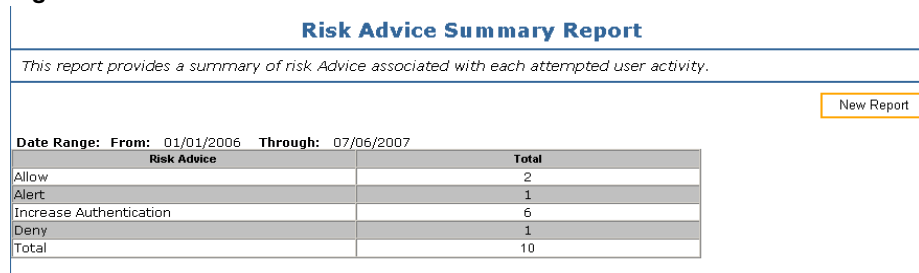
## Risk Advice Summary Report

RiskFort Advice Summary Report provides an overall summary of advices that were returned by the RiskFort over the specified period of time.

**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.

The following figure displays a Risk Advice Summary Report page.

**Figure 4-11**



The following table lists the information included in a RiskFort Advice Summary Report:

**Table 4-9** Risk Advice Summary Report Fields

| Fields             | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Risk Advice</b> | The advice given by RiskFort for every transaction: <ul style="list-style-type: none"> <li>• <b>Allow</b>- Allow the transaction to proceed.</li> <li>• <b>Increase Authentication</b> - Must perform secondary or additional authentication before proceeding any further.</li> <li>• <b>Alert</b>- Alert and create user, if required.</li> <li>• <b>Deny</b>- Deny the transaction from proceeding.</li> </ul> |
| <b>Total</b>       | The total number of transactions.                                                                                                                                                                                                                                                                                                                                                                                 |

To generate an Risk Advice Summary Report, perform the following tasks:

1. Under **Reports** menu on the left-hand, click **Risk Advice Summary Report**.

The Risk Advice Summary Report page is displayed.

2. Select the **Date Range** from the drop-down menu. You can also select a pre-defined date range in the **From** and **Through** fields.

The summary of the report is displayed.

## Risk Evaluation Detail Activity Report

This report shows all transactions performed by the RiskFort Server.

The following figure displays a Risk Evaluation Detail Activity Report page.

**Figure 4-12**

| Risk Evaluation Detail Activity Report                                                                                                              |          |                   |              |            |             |                   |             |                  |                       |            |           |                            |        |                 |        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------------------|--------------|------------|-------------|-------------------|-------------|------------------|-----------------------|------------|-----------|----------------------------|--------|-----------------|--------|
| <i>This report displays all risk-related activity, related user activity.</i>                                                                       |          |                   |              |            |             |                   |             |                  |                       |            |           |                            |        |                 |        |
| Events to Display <input type="button" value="All Events"/>                                                                                         |          |                   |              |            |             |                   |             |                  |                       |            |           |                            |        |                 |        |
| User name used for search is : Date Range: From: 01/01/2007 Through: 08/09/2007<br>1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 [Next>>] Last |          |                   |              |            |             |                   |             |                  |                       |            |           |                            |        |                 |        |
| Date                                                                                                                                                | Username | Event Type        | Event Status | Risk Score | Risk Advice | Bypass Evaluation | Negative IP | Negative Country | Trusted Aggregator IP | User Known | Device Id | Machine Finger Print Check | Group  | Credential Type | Action |
| 08/07/2007 19:29:17                                                                                                                                 | JCHOI    | Update Attributes | Failure      | N/A        | N/A         | N/A               | N/A         | N/A              | N/A                   | N/A        | N/A       | N/A                        | GROUP2 | N/A             | N/A    |
| 08/07/2007 19:29:17                                                                                                                                 | JCHOI    | Update Attributes | Failure      | N/A        | N/A         | N/A               | N/A         | N/A              | N/A                   | N/A        | N/A       | N/A                        | GROUP2 | N/A             | N/A    |
| 08/07/2007 19:29:17                                                                                                                                 | JCHOI    | Update Attributes | Failure      | N/A        | N/A         | N/A               | N/A         | N/A              | N/A                   | N/A        | N/A       | N/A                        | GROUP2 | N/A             | N/A    |
| 08/07/2007 19:28:07                                                                                                                                 | JCHOI    | Evaluate risk     | Success      | 50         | Alert       | No                | No          | No               | No                    | No         | Not Found | No                         | GROUP2 | ARCOTID         | LOGIN  |

The following table lists the information included in a Risk Evaluation Detail Activity

**Table 4-10** Risk Evaluation Detail Activity Report Fields

| Fields                | Description                                                                                                                                                                                                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Date                  | The timestamp when risk evaluation was done for the user.                                                                                                                                                                                                                                             |
| Username              | The unique user name.                                                                                                                                                                                                                                                                                 |
| Event Type            | The type of risk evaluation activity that was performed by RiskFort Server. These activities include: <ul style="list-style-type: none"> <li>• Evaluate risk</li> <li>• Update attributes</li> <li>• Create associations</li> <li>• Delete associations</li> </ul>                                    |
| Event Status          | The status of the event action taken and can be: <ul style="list-style-type: none"> <li>• <b>Success</b> - RiskFort was able to perform the risk evaluation activity successfully.</li> <li>• <b>Failure</b> - RiskFort was not able to perform the risk evaluation activity successfully.</li> </ul> |
| Risk Score            | The score generated for the given transaction.                                                                                                                                                                                                                                                        |
| Risk Advice           | The advice given by the RiskFort application depending on the score generated. The advice can be: <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> <li>• Alert</li> <li>• Increase Authentication</li> </ul>                                                                       |
| Exception User        | Whether the user is in Exception User List or not.                                                                                                                                                                                                                                                    |
| Negative IP           | Whether the Negative IP rule was applied or not. In case it was applied, then <b>Yes</b> or <b>No</b> 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 <b>Yes</b> or <b>No</b> indicate whether rule returned a match or not.                                                                                                                                             |
| Trusted Aggregator IP | Whether the Trusted Aggregator IP rule was applied or not. In case it was applied, then <b>Yes</b> or <b>No</b> indicate whether rule returned a match or not.                                                                                                                                        |
| User Known            | Whether the user is enrolled in the system or not.                                                                                                                                                                                                                                                    |
| Device ID             | The result of the user Device ID check.                                                                                                                                                                                                                                                               |

**Table 4-10** Risk Evaluation Detail Activity Report Fields

| Fields                     | Description                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Machine Finger Print Check | The machine finger print check for the user passed.                                                                                                                                                                                         |
| Group                      | The group to which user belongs.                                                                                                                                                                                                            |
| Credentials                | The type of credential with which user authentication was done. Currently, only ArcotID credential is shown.                                                                                                                                |
| Action                     | The status of the action taken. Action status can be: <ul style="list-style-type: none"> <li>• <b>Success</b> - If the action was completed successfully.</li> <li>• <b>Failure</b> - If the user failed to complete the action.</li> </ul> |
| Caller Id                  | A unique identifier passed to RiskFort APIs by the calling application. Caller ID can be blank, if the calling application does not set the value.                                                                                          |
| Event Id                   | The internal unique ID provided by RiskFort Server for each activity performed by it.                                                                                                                                                       |
| Instance Id                | The unique identifier of every instance of RiskFort Server, in case multiple instances are deployed in an installation.                                                                                                                     |

To generate a Risk Evaluation Detail Activity Report, perform the following steps:

1. Under **Reports** menu on the left-hand, click **Risk Evaluation Detail Activity Report**.

The Risk Evaluation Detail Activity Report page is displayed, as shown in the following figure.

**Figure 4-13**

The screenshot shows the Arcot RiskFort Administration interface. On the left is a sidebar menu with the following items: Admin Configurations, WebFort Configurations, Issuance Configurations, SignFort Configurations, RiskFort Configurations, Reports (selected), Administrator Activity Audit Report, Credential Management Report, Authentication Activity Report, Signing Activity Report, Digital ID Management Report, RiskFort Trusted Aggregator Report, RiskFort Negative IP Report, RiskFort Exception User Report, Risk Advice Summary Report, RiskFort Negative Country Report, and Risk Evaluation Detail Activity Report. The main content area is titled 'Risk Evaluation Detail Activity Report' and includes a subtitle 'Select the period for viewing risk evaluation activity.' Below this, there are filters for 'Date Range' (set to 'Custom'), 'From' (11/08/2007), 'Through' (11/08/2007), 'Group' (ADMINISTRATORS), and 'User Name' (empty). There are 'Clear' and 'Display Report' buttons at the bottom of the filter section. The top right of the page shows the user 'Welcome admin | Global Admin' and the 'Last Login Time 11/08/2007 07:04:40 AM GMT'. There are also links for 'User Profile' and 'Logout'.

2. Select the **Date Range** from the drop-down menu.

You can also select a pre-defined date range in the **From** and **Through** fields.

3. If required, enter the name of an administrator in the **User Name** field for further filtering the data.
4. Select one of the following groups from the **Group** drop-down menu:
  - **ADMINISTRATORS**: Refers to administrators' group.
  - **GROUP2**: Refers to users of the group.

**NOTE:** The Group drop-down menu appears only if the administrator performing this activity has privileges for more than one group.

5. Click **Display Report** to view the generated report.
6. Click **Export** to save the report to a file.

For more information on how to export reports, refer to the section [“Exporting Reports to a File.”](#)

# Exporting Reports to a File

Reports can be exported to a Comma-Separated Value (CSV) file. The exported report can be later opened in a spreadsheet (for example, Microsoft Excel) for any data manipulation. This feature is very useful if post-processing or sorting of reports is required.

To export a report to a file, perform the following tasks:

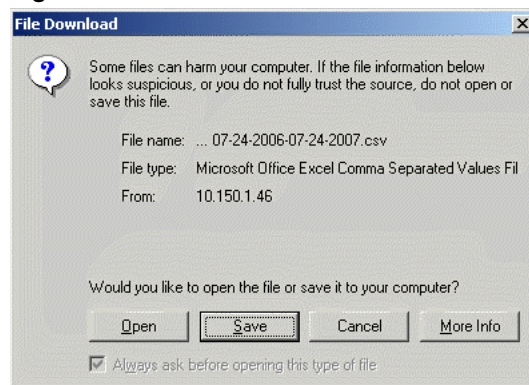
1. Click the desired report link.

The report criteria page for the selected report is displayed.

2. Select the **Date Range** from the drop-down menu, select a predefined date range in the **From** and **Through** fields, and enter a **User Name**.
3. Click **Display Report** to view the report generated for the administrator.
4. Click **Export** to save the file.

The File Download page is displayed, as shown in the following figure.

**Figure 4-14**



5. Read the information displayed in the page.
6. Click **Save** to save the file. This file can later be viewed by using a spreadsheet application, such as Microsoft Excel.

## Chapter 5

# 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)
- `arversion` (RiskFort Modules Version Display Tool)
- `aradmin` (RiskFort Server Refresh and Shutdown Tool)
- `arrfupload` (Arcot RiskFort Data Upload Tool)

# dbutil (RiskFort Database Tool)

After RiskFort is installed, the `securestore.enc` file is created at the following location:

- On Windows

`<install_location>\Arcot Systems\conf\`

- On UNIX-based Platforms

`<install_location>/arcot/conf/`

This file stores the following information that you need to connect to the database in encrypted format:

- Master key name
- Database user name and password
- Database values

The `dbutil` tool allows you to edit the `securestore.enc` file to:

- [Set Up the Master Key](#)
- [Insert a Database User Name and Password](#)
- [Use Additional dbutil Options](#)

## Set Up the Master Key

The *Master Key* is specified during the installation and is used to encrypt the values in the `securestore.enc` file. It also encrypts all encryption keys that are stored in the database.

If for some reason you need to change the Master Key value in `securestore.enc`, then:

**CAUTION:**THE FOLLOWING PROCEDURE MUST BE DONE ONLY IF THE MASTER KEY SETUP FAILED DURING THE INSTALLATION. CONTACT ARCOT TECHNICAL SUPPORT FOR HELP.

1. Backup the current `securestore.enc` file.
2. Delete the `securestore.enc` file.
3. Run the following command:

**dbutil -init MasterKey**

The dbutil tool re-creates `securestore.enc` in the following location with the master key name:

**On Windows**

```
<install_location>\Arcot Systems\conf\
```

**On UNIX  
Platforms**

```
<install_location>/arcot/conf/
```

## 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.

**NOTE:** DSN/password are used by servers, while username/password are used by Java components.

The `dbutil insert` option adds the required values to the file instead of overwriting or updating them.

To insert the database user name and password in the `securestore.enc` file, 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 Database user name. For example:

```
dbutil -pi ArcotDSNName manager
```

The `dbutil` tool inserts the Database user name and password values in the `securestore.enc` file.

## Use Additional dbutil Options

The following table lists the additional options for `dbutil`. In this table, *key/value* pair refers to either DSN, password, or database user name/password pair.

**Table 5-1** Additional dbutil Options

| Option           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-pd</code> | <p>Deletes the specified key/value pair from <code>securestore.enc</code>.</p> <p>Syntax:</p> <pre>dbutil -pd key</pre> <p>For example:</p> <pre>dbutil -pd RiskFortDatabaseDSNold</pre>                                                                                                                                                                                                                                                                                                                 |
| <code>-pi</code> | <p>Inserts an additional key/value pair into <code>securestore.enc</code> (as discussed in the previous section, <a href="#">“Insert a Database User Name and Password,”</a>).</p> <p>Syntax:</p> <pre>dbutil -pi key value</pre> <p>For example:</p> <pre>dbutil -pi RiskFortBackupDSN dbapass-<br/>word</pre> <p>Each key can only have one value. If you have already inserted a key/value pair, you cannot insert another value for the same key. To change a key's value, use <code>-pu</code>.</p> |
| <code>-pu</code> | <p>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.</p> <p>Syntax:</p> <pre>dbutil -pu key value</pre> <p>For example:</p> <pre>dbutil -pu RiskFortDatabaseDSN newPass-<br/>word</pre>                                                                                                                                                                                                          |

# arversion (RiskFort Modules Version Display Tool)

The `arversion` tool enables you to check and display the version information of the modules provided by Arcot. These modules are provided as `.dll` files on Windows and `.so` on UNIX-based platforms.

**NOTE:** In case of deployment-related problems, when you contact Arcot Technical Support, you might need to specify the version of the deployed modules.

The syntax to use the tool is:

```
arversion <library1_path> [<library2_path> ...]
```

In the preceding syntax, the `<libraryN_path>` string specifies the name of individual module. For example:

- `aradminprotocol.dll` on Windows
- `libaradminprotocol.so` on UNIX-based platforms

If you do not specify the absolute path of the library module, then the 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:

```
arversion <install_location>\Arcot
Systems\plugins\protocols\aradminprotocol.dll
```

## UNIX-based Platforms:

```
arversion
<install_location>/arcot/plugins/protocols/libaradminprotocol.so
```

# aradmin (RiskFort 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 to be restarted. In the latter case, the current Administration Console informs you to refresh or restart, as applicable.

The refresh option ensures that the server does not take any down time. Very few configuration changes need the server to be restarted.

The `aradmin` tool enables you to gracefully shut down the server. In case of graceful shutdown, server allows all existing requests to complete while not accepting any new requests.

The syntax to use the tool is:

```
aradmin <server_ip> <server_port> <options>
```

The following table lists the parameters used by the `aradmin` tool.

**Table 5-2** aradmin Parameters

| Parameters               | Description                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>server_ip</code>   | IP address or the host name at which the RiskFort Server is available.                                                                                       |
| <code>server_port</code> | Port number at which the RiskFort Server listens to the operations requests.<br><br><b>NOTE:</b> The default <code>server_port</code> value is <b>7980</b> . |

The following table lists the options supported by the `aradmin` tool.

**Table 5-3** aradmin Options

| Options         | Description                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-d</code> | This option is used to initiate the graceful shutdown of the server.<br><br>For example:<br><br><code>aradmin 10.150.1.40 7980 -d</code> |

**Table 5-3** aradmin Options

| Options | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r      | <p>This option is used to send a refresh request to the server.</p> <p>For example:</p> <pre>aradmin 10.150.1.40 7980 -r</pre> <p>To refresh a log level, the refresh option is used as follows:</p> <pre>aradmin &lt;server_ip&gt; &lt;server_port&gt; -r log:all=&lt;log_level&gt;</pre> <p>The possible values for log_level are:</p> <ul style="list-style-type: none"> <li>• 0 FATAL</li> <li>• 1 WARNING</li> <li>• 2 INFO</li> <li>• 3 DETAIL</li> </ul> |

## Configuring for TLS-Based Communication

To configure **aradmin** tool for TLS-based communication, you must perform the following steps:

1. [Edit arcotcommon.ini](#)
2. [Configure Server Management Protocol](#)

### Edit arcotcommon.ini

If RiskFort Server is configured for TLS transport mode, then you *must* add the following section to **arcotcommon.ini** file:

```
[arcot/aradmin/tlsconfig]
ServerCACert=<CA certificate(PEM) file path>
```

Set the parameter ServerCACert to the CA certificate file path. The file *must* be in . PEM format. For example:

```
ServerCACert=<install_location>/Arcot
Systems/certs/riskfort_ca.pem
```

**IMPORTANT:** The private 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 Server Management Protocol

To configure RiskFort Server Management protocol for TLS:

1. Log in to the Administration Console.
2. Under **RiskFort Configurations** from the side-bar menu, select **Protocol Setup**.

The RiskFort Protocol Setup page appears.

3. Perform the following steps to configure the RiskFort Server Management protocol for TLS:
  - a. In the **Enable** column, ensure that the check box for **Server Management** protocol to be enabled for TLS is selected.
  - b. In the **Transport Security** column, select **TLS** from the drop-down list.
  - c. In the **SSL/TLS 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.

- d. Click **Save** to save the changes.
4. Restart RiskFort Server.
5. Restart the application server.

# arrfupload (Arcot RiskFort Data Upload Tool)

RiskFort uses Quova data to identify the geolocation 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 47, “Configuring Negative IP Address List” on page 49, “Configuring Velocity Check” on page 51, and “Configuring Zone Hopping Check” on page 54 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](mailto: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.

This tool is available at the following location:

**On Windows:** C:\Program Files\Arcot Systems\bin\

**On UNIX  
Platforms:** \$ARCOT\_HOME/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.

Run the following command to use the tool:

**On Windows:** C:\Program Files\Arcot Systems\bin\arrfupload.exe <option>

**On UNIX  
Platforms:** \$ARCOT\_HOME/arcot/bin/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 `aradmin <server_ip> <server_port> -r` command.

The following table lists the options supported by the utility.

**Table 5-4** aradmin Options

| Options | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -config | <p>This option is used to read information from <b>riskfortdataupload.ini</b> (the configuration file used by the tool) and perform the required action.</p> <p>This option uses the following flags:</p> <ul style="list-style-type: none"> <li>• <b>Tables:</b> The set of tables the user wants to update. The values allowed are either Geopoint or Anonymizer. If neither is specified, then no data is uploaded. This option does not have any default value.</li> <li>• <b>Load:</b> If set to 1, indicates that the data will be uploaded and if set to 0 indicates that data will not be uploaded. The default is value is 0.<br/><br/><b>IMPORTANT:</b>If set to 1, the Filename and Tables flags <i>must</i> be set.</li> <li>• <b>Swap:</b> If set to 1, indicates that the table will be swapped and if set to 0 indicates that table will not be swapped. The default is value is 0.<br/><br/><b>IMPORTANT:</b>This flag is valid only if the Tables flag is set correctly. Also, you must refresh the RiskFort Server cache to be able to use the new table.</li> <li>• <b>Filename:</b> Indicates the name and the path of the Quova file that contains the data to be uploaded.<br/><br/><b>IMPORTANT:</b>This flag is valid only if the Load flag is set to 1.</li> </ul> |
| -tnames | <p>This option is used to display the current ARQGeoPoint and ARQ-GeoAnonymizer tables being used by the RiskFort database.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 5-4** aradmin Options

| Options | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -prompt | <p>This option is used to display an interactive command-line menu that enables the user to select the table (<b>ARQGeoPoint</b> or <b>ARQAnonymizer</b>) they want to update using the latest Quova data. Based on the table specified by the user, a sub-menu with following options appears:</p> <ul style="list-style-type: none"> <li>• <b>Load Quova Data:</b> 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.</li> <li>• <b>Swap Quova Tables:</b> Depending on the set of tables chosen from the main menu, enables the user to swap tables.</li> <li>• <b>Exit to the previous menu:</b> Enables the user to the main menu.</li> <li>• <b>Exit the program:</b> Enables the user to exit from the tool.</li> </ul> |

### Improving the Performance of Database Lookup While Using the Tool

The RiskFort Data Upload Tool can be used to upload geolocation data (mapping between IP addresses and geographic location) to the ARQGeoPoint1 or ARQGeoPoint2 table, depending on your current configuration. To find the geographic location for a given IP address, RiskFort needs to look up these tables during a transaction.

Because the number of records in these tables can be very high, this look-up time can be proportionally high, if the database is not tuned properly. Arcot recommends that you use the following command *after every upload* of geolocation data from Quova to improve the performance:

**NOTE:** If the database performance is still not good, contact your DBA to tune the database.

```
Analyze table <table_name> compute statistics;
```

In the preceding command, *table\_name* represents ARQGeoPoint1 or ARQGeoPoint2.

### riskfortdataupload.ini

The **riskfortdataupload.ini** file controls the behavior of the Arcot RiskFort Data Upload tool. It is available at the following location:

**On Windows:** C:\Program Files\Arcot Systems\conf\

**On UNIX  
Platforms:**

`$ARCOT_HOME/arcot/bin/conf/`

The following table lists the configuration parameters in this file.

**Table 5-5** Configuration Parameters for riskfortdataupload.ini

| Parameter | Default     | Description                                                                                                                                                               |
|-----------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tables    | Do Not Load | The tables that the user can work with.<br>Possible values are: <ul style="list-style-type: none"> <li>ARQGeoPoint</li> <li>ARQAnonymizer</li> </ul>                      |
| Load      | 0           | The indicator whether to upload the data to the table or not.<br>Possible values are: <ul style="list-style-type: none"> <li>0 (Do not load)</li> <li>1 (Load)</li> </ul> |
| Swap      | 0           | The indicator whether to swap the tables or not.<br>Possible values are: <ul style="list-style-type: none"> <li>0 (Do not swap)</li> <li>1 (Swap)</li> </ul>              |
| Filename  | --          | The name of the file from which the Quova data has to be loaded.<br><b>IMPORTANT:</b> 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.

### Sample riskfortdataupload.ini

This section provides the content of the default configuration files that appear after installation.

```
#-----#

#ini file for Quova data upload
[arcot/riskfort/dataupload]
The set of tables to work with:
Allowed values are: ARQGeoPoint(Use ARQGeopoint tables),
ARQAnonymizer(Use ARQAnonymizer tables)
```

```

Default: Do not Load
Tables=ARQGeoPoint

This flag indicates whether to load the table with data or
not.
Allowed values are: 0 (Do not load), 1 (Load)
Default: 0
Load=1

This flag indicates whether to swap the tables or not
Allowed values are: 0 (Do not swap), 1 (Swap)
Default: 0
Swap=1

This flag gives the name of the file from which the Quova
data has to be loaded
The filename along with the absolute path where the file is
located should be mentioned in the flag
For example
For Windows - Filename=C:\My
Documents\Quova\EDITION_Media_2006-08-10_with_v270.dat
For Unix -
/opt/quova/EDITION_Media_2006-08-10_with_v270.dat
Filename=

The logfilename is generated automatically by the RiskFort
Upload Tool at the same place as the "arcotriskfort.log"
file with the name starting with arcotriskfortuploadtool
followed by the date and time at which the tool was started.
The date/time appended is according to Greenwich Mean Time
(GMT).
The logging configuration can be done for RiskFort Upload
Tool using riskfortserver.ini which is used by the RiskFort
Server.
For this tool, only the following three fields can be
configured:
1. LogFileSize
2. BackupLogFileDir
3. LogLevel
#-----#

```



## Appendix A

# Working with Sample Callouts

RiskFort 1.7 is shipped with a basic non-GUI Sample Callouts WAR file (**riskfort-1.7-sample-callouts.war**) that demonstrates:

- Basic operations (invocation and post-processing) of RiskFort Server from your custom program.
- 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 appendix covers:

- [Deploying Sample Callouts](#)
- [Configuring RiskFort Server to Communicate With Sample Callouts](#)
- [Using 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-1.7-sample-callouts.war` file on *from* the following location:

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

**NOTE:** Although you will also see `riskfort-1.7-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. Start the application server services.

**IMPORTANT:** If you are using IBM WebSphere, then you must restart the WebSphere server.

## 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-1.7-sample-application.war` file *from* the following location:

```
<install_location>/arcot/samples/java/
```

**NOTE:** Although you will also see `riskfort-1.7-sample-application.war` in the package, it is recommended that you deploy the Sample Application WAR file from the preceding location.

3. Start the application server services.

**NOTE:** If you are using IBM WebSphere, then you must restart the WebSphere server.

## Configuring RiskFort Server to Communicate With Sample Callouts

To configure the Sample Callouts, perform the following steps:

1. Under **RiskFort Configurations** on the side-bar menu, select **Callout Configuration**.

The Callout Configuration page appears.

2. In the **Evaluation Callout Configuration** table, under the **PROPOSED** column:

- 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 **URL of Callout** option:

<http://<host>:<port>/riskfort-1.7-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 **Receive 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. Repeat the sub-steps in **Step 2** for **Scoring Callout Configuration** table.

Specify the following against the **URL of Callout** option:

<http://<host>:<port>/riskfort-1.7-sample-callouts/SampleScoringCalloutServlet>

4. Under **RiskFort Configurations** on the side-bar menu, select **Scoring Configuration**.

The Scoring Configuration page appears.

5. In the **Enable or Disable Scoring Callout** table, under the **PROPOSED** column:
  - a. Select **Enable Scoring Callout**.
  - b. 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.

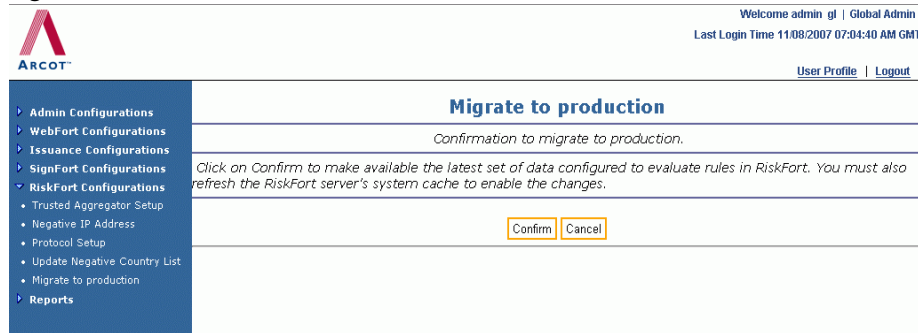
6. To make the changes active, you must migrate them to production:
  - a. Under **RiskFort Configurations** on the side-bar menu, select **Migrate to Production**.

The Migrate to Production page appears.

- b. Click **Migrate**.

The page to confirm the action is displayed, as shown in the following figure.

**Figure A-1**



- c. On the confirmation page, click **Confirm** to start the migration process.

The "Migrated to production successfully." message is displayed.

**NOTE:** Ensure that you refresh the server cache after you complete the migration.

7. Run the **aradmin** tool to refresh the RiskFort Server as follows:
  - a. Navigate to the following directory:

**On Windows:** `<install_location>\Arcot Systems\bin\`

**On UNIX  
Platforms:** `<install_location>/arcot/bin/`

- b. Run the following command:

```
aradmin <server_ip> <server_port> -r
```

8. Restart the RiskFort Server.

## Using 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-1.7-sample-application/index.jsp
```

The RiskFort Sample Application page appears.

2. Create a new user by clicking **User Creation**.
3. After the user has been created, return to the RiskFort Sample Application page by clicking **Main Page**.
4. Click **Risk Evaluation** 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.

5. Return to the RiskFort Sample Application page by clicking **Main Page**.
6. Edit the Sample Callout `ScoringCalloutResponse.xml` file:

- a. Navigate to **ScoringCalloutResponse.xml** file.

In case of Apache Tomcat, this file is available at:

```
<AppHome>/riskfort-1.7-sample-callouts>/WEB-INF/classes/
```

- b. Open the file in an editor window and edit the value (85) for the **<Score>** element to a desired value.

- c. Save the change.
7. Restart the application server.
8. Restart RiskFort Server.
9. Repeat [Step 2](#) through [Step 4](#).

The Risk Score will now reflect the change you made in `ScoringCalloutResponse.xml` the file. The Risk Advice will reflect the change in the Risk Score.

# Glossary

|                                               |                                                                                                                                                                                                                                      |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aggregator</b>                             | Third-party vendors who provides account aggregation services by collating user information across multiple enterprises.                                                                                                             |
| <b>Add-On Rule</b>                            | Additional Risk Evaluation rule that ships with RiskFort.                                                                                                                                                                            |
| <b>aradmin</b>                                | Arcot proprietary tool for refreshing and gracefully shutting down the RiskFort Server.                                                                                                                                              |
| <b>arversion</b>                              | Arcot proprietary tool for checking and displaying the version information of Arcot modules.                                                                                                                                         |
| <b>Authentication</b>                         | A process by which an entity proves that it is who it claims to be.                                                                                                                                                                  |
| <b>Authentication Token</b>                   | A token is an object that an authorized user of computer services is given to aid in authentication.                                                                                                                                 |
| <b>Callout</b>                                | Custom program executing externally (outside RiskFort).                                                                                                                                                                              |
| <b>Callout Framework</b>                      | Component of RiskFort Server that handles <a href="#">Callouts</a> .                                                                                                                                                                 |
| <b>Certificate</b>                            | See <a href="#">Digital Certificate</a> .                                                                                                                                                                                            |
| <b>Credential</b>                             | 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.                                                                 |
| <b>Customer Support Representatives (CSR)</b> | Administrators responsible for the day-to-day operations related to users of the security system.<br><br>For example, Administrators can assist users with enrollment, resetting users passwords, and generating enrollment reports. |
| <b>dbUtil</b>                                 | Arcot proprietary tool for managing encrypted information to connect to the RiskFort database.                                                                                                                                       |
| <b>Device Velocity</b>                        | Number of transactions from the same device within a specified time.                                                                                                                                                                 |
| <b>Digital Certificate</b>                    | 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.                         |

|                                        |                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Encryption</b>                      | The process of scrambling information in a way that disguises its meaning.                                                                                                                                                                                                                                                            |
| <b>Exception User</b>                  | User “known” to RiskFort and is excluded from risk assessments for a specified period of time.                                                                                                                                                                                                                                        |
| <b>Evaluation Callout</b>              | <b>Callout</b> that runs after all <b>Evaluation Rules</b> and contains custom risk evaluation logic.                                                                                                                                                                                                                                 |
| <b>Evaluation Rule</b>                 | Pre-configured RiskFort logic that is applied to the incoming transaction data.                                                                                                                                                                                                                                                       |
| <b>Extensible Element</b>              | Additional element pertaining to a transaction that is used by <b>Add-On Rules</b> for risk evaluation.                                                                                                                                                                                                                               |
| <b>Global Administrator</b>            | An administrator responsible for setting up <b>Customer Support Representatives (CSR)</b> accounts and configuring the system.                                                                                                                                                                                                        |
| <b>Increased Authentication</b>        | <p>The <b>Risk Advice</b> given by RiskFort, if the current transaction is considered unsafe by RiskFort.</p> <p>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.</p> |
| <b>Master Administrator</b>            | The highest level of RiskFort administrator, whose primary responsibilities are to initialize RiskFort and create Global Administrator accounts.                                                                                                                                                                                      |
| <b>Negative IP Address</b>             | IP address that has been the origin of known anonymizer proxies or fraudulent or malicious transactions in the past.                                                                                                                                                                                                                  |
| <b>Negative Country</b>                | Country from which fraudulent or malicious transactions are known to have originated in the past.                                                                                                                                                                                                                                     |
| <b>Non-Terminating Rule</b>            | The rule alone does not determine overall <b>Risk Score</b> . It requires other rules for the purpose.                                                                                                                                                                                                                                |
| <b>One-Way SSL</b>                     | Client application verifies the identity of the server application (by accepting server’s <b>Digital Certificate</b> ) before the SSL session is established.                                                                                                                                                                         |
| <b>Private Key</b>                     | One of a pair of keys used in PKI, which is kept secret and can be used to decrypt or encrypt data.                                                                                                                                                                                                                                   |
| <b>Public Key</b>                      | <p>One of a pair of keys used in PKI, which is distributed freely and is published as part of a certificate.</p> <p>It is typically used to encrypt data sent to the public key’s owner, who then decrypts the data using the corresponding private key.</p>                                                                          |
| <b>Public Key Infrastructure (PKI)</b> | The standards and services that facilitate the use of public-key cryptography and certificates in a networked environment.                                                                                                                                                                                                            |

|                                            |                                                                                                                                                                                |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RiskFort</b>                            | RiskFort provides a mechanism to evaluate the risk of a given transaction.                                                                                                     |
| <b>Risk Advice</b>                         | An action (ALLOW, ALERT, DENY, INCREASEAUTH) suggested by RiskFort to the calling application, after evaluating the risk of an transaction.                                    |
| <b>RiskFort Native Protocol</b>            | Arcot proprietary protocol for communication between RiskFort Server, its components, WebFort Server, and Administration Console.                                              |
| <b>Risk Score</b>                          | 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.                      |
| <b>Scoring Callout</b>                     | <b>Callout</b> that runs after scoring by RiskFort's <b>Scoring Engine</b> and contains custom scoring logic to modify final <b>Risk Score</b> .                               |
| <b>Scoring Engine</b>                      | Component of RiskFort Server that collects <b>Risk Scores</b> from individual <b>Evaluation Rules</b> and processes them in the order of the scoring precedence.               |
| <b>Scoring Rule</b>                        | Last Rule that receives execution results of all other configured rules and returns the final <b>Risk Score</b> and <b>Risk Advice</b> .                                       |
| <b>Server Management Protocol</b>          | Arcot proprietary protocol for starting and shutting down the RiskFort Server.                                                                                                 |
| <b>Secure Sockets Layer (SSL)</b>          | Protocol for managing the security of a message transmission on public networks.<br><br>This protocol is predecessor of <b>Transport Layer Security (TLS)</b> .                |
| <b>Terminating Rule</b>                    | The rule that alone determines overall <b>Risk Score</b> .                                                                                                                     |
| <b>Transmission Control Protocol (TCP)</b> | Internet protocol for guaranteed transmission of data. It sends data unencrypted.                                                                                              |
| <b>Transport Layer Security (TLS)</b>      | Protocol to secure and authenticate communications across public networks by using data encryption.                                                                            |
| <b>Trusted Aggregator</b>                  | Aggregator "trusted" to the organization and, therefore, excluded from future risk assessments.                                                                                |
| <b>Trusted IP Address</b>                  | IP address that is "trusted" and, therefore, excluded from future risk evaluations.                                                                                            |
| <b>Two-Way SSL</b>                         | Both, client application and the server application verify each other's identity (by presenting respective <b>Digital Certificate</b> ) before the SSL session is established. |
| <b>UserID/Password</b>                     | One of the credential issued to the user during enrollment.                                                                                                                    |

|                       |                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>User Velocity</b>  | Number of transactions from the same user within a specified time.                                                      |
| <b>Velocity Check</b> | See <a href="#">Device Velocity</a> and <a href="#">User Velocity</a> .                                                 |
| <b>Zone Hopping</b>   | Successive transactions (from same user) separated by a distance of more than what a reasonable user-speed can achieve. |

# Index

## A

- active data 51
- Add-On rules 59
- Administration Console 1
  - interface 2
  - logging in 9
- administrative tasks 8
  - changing password 10
  - creating administrator accounts 12
    - CSR account 15
    - Global administrator 12
  - deleting administrator account 21
  - enabling administrator accounts 20
  - updating administrator policies 18
- administrator levels 4
  - Global Administrator 5
  - Master Administrator 4
- Advice 57
- aggregators 38
- annotation string 60
- Arcot RiskFort Data Upload Tool 109

## B

- base elements 63

## C

- Callout 68
  - Evaluation 60
  - Scoring 60
- Combination rules 59
- configuration
  - negative IP address list 49
  - migrating to production 78
  - negative country list 51

- protocol setup 27
- trusted aggregators 38

## D

- DBUtil
  - inserting userID and password 103
  - options 104
- device signature 32
- disabling administrator accounts 20

## E

- Evaluation Callout 60
- Exception user 59
- Exception User List 59
- exporting reports
  - to a file 100
- Extensible elements 63

## F

- features
  - sample Risk Advice matrix 57

## I

- intended audience iii

## L

- logging out 9

## M

- Machine FingerPrint 32
- master key 102
- MFP 32

modifier string 60

## N

Negative Country list 45  
Negative IP address list 49  
non-terminating rules 60

## R

reports 81  
    administrator activity audit report 82  
    configuration data reports 87  
    transaction reports 95  
Risk Advice 57  
Risk Advice Matrix 57  
Risk Score 57  
Rule types 57  
    Evaluation  
        Standalone 58  
        Add-On 59  
        Built-in 59  
        Combination 59  
    Scoring 60  
    terminating 58  
rules  
    non-terminating 60

## S

Score 57  
Scoring Callout 60  
Scoring Rules 60  
securestore.enc 103  
staging data 51  
Standalone rules 58  
system administration tools 101  
    aradmin 106  
    arversion 105  
    dbutil 102

## T

terminating rules 58  
Trusted IP address list 34

## U

user creation mode 32  
    explicit 32  
    implicit 32

## V

Velocity check 51  
    Device Velocity 51  
    User Velocity 51

## Z

Zone hopping 54