CA RiskMinder™

Administration Guide

r3.1.01

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Overview of the Administration Console 13

About the Administration Console 14
Elements of the Administration Console 15
Supported Roles 16
- Users 16
- Default Administrative Roles 17
- Custom Roles 23

Next Steps: Quick Administration 23
- For Simple Deployments 24
- For Complex Deployments 26

Chapter 2: Getting Started 29

Accessing the Administration Console 30
Changing Password and Profile Information 31
Configuring Administration Console Settings 32
- Updating UDS Configurations 32
- Refreshing the Cache 37
- Viewing the Status of Cache Refresh Requests 39
- Configuring Attribute Encryption 41
- Configuring Custom Locales 43
- Setting the Default Organization 44
- Configuring the Account Type 45
- Configuring Email and Telephone Type 48
- Specifying Basic Authentication Policy Settings 49
- Specifying Master Administrator Authentication Policy Settings 51
- Configuring Web Services Authentication and Authorization 53

Chapter 3: Working with Custom Roles 55

Understanding Custom Roles 55
- Things That You Should Know About Custom Roles 56
- Pre-Defined Custom Roles 56

Creating a Custom Role 57
Updating Custom Role Information 58
Deleting a Custom Role 59
Summary of Administrative Privileges 59

Chapter 4: Managing RiskMinder Server Instances 65

Configuring Server Connectivity 66
RiskMinder Server Management Connectivity 67
Case Management Queuing Server Management Connectivity 68
RiskMinder Administration Connectivity 69
Case Management Queuing Server Connectivity 70
Creating Trust Stores 71
Configuring Communication Protocols 72
(Optional) Configuring SSL Communication 76
Configuring the RiskMinder Predictive Model 77
Refreshing a Server Instance 77
Using Administration Console to Refresh Server Instances 78
Using the arrfclient Tool to Refresh Server Instances 80
Updating Server Instance Configurations 81
Shutting Down a Server Instance 83
Restarting a Server Instance 84

Chapter 5: Configuring SSL 85

RiskFort Components and Their Communication Modes 86
Prepare for SSL Communication 87
Obtaining Certificates Directly Through a Certificate Authority (CA) 88
Generating Certificate Requests by Using a Utility 92
Enable SSL Between RiskMinder Server and User Data Service 93
One-Way SSL 94
Two-Way SSL 95
Enable SSL Between Case Management Queuing Server and User Data Service 96
One-Way SSL 96
Two-Way SSL 97
Enable SSL Between Administration Console and RiskMinder Server 97
For Server Refresh, Restart, Instance Management, and Protocol Management Activities 98
For Rule Configurations Activities 103
Enable SSL Between Administration Console and Case Management Queuing Server 108
For Server Refresh and Restart Activities 108
For Fetching Cases 113
Enable SSL Between Java SDK and RiskMinder Server 118
One-Way SSL 119
Two-Way SSL 121
Enable SSL Communication Between Risk Evaluation Web Service and RiskMinder Server 123
One-Way SSL 124
Two-Way SSL 125
Enable SSL Communication Between Administration Web Service and RiskMinder Server 126

One-Way SSL 127
Two-Way SSL 128
Enable One-Way SSL Between RiskMinder Components and Database 129
Between RiskMinder Server and Database 129
Between Administration Console and Database 131
Between UDS and Database 131

Chapter 6: Understanding RiskMinder Rule Basics 133

Evaluation Rules 135
Out-of-the-Box Rules 135
New Rules Added Using the Rule Builder 137
Evaluation Callout 137
Scoring Engine 137
Scoring Callout 138

Chapter 7: How to Build a Custom Rule 138

Create the Safe Countries Rule 141
Upload Data for the Safe Countries Rule 142
Create the High User Velocity from Unexpected Locations Rule 143
Deploy the High User Velocity from Unexpected Locations Rule 144
Migrate Rules to Production 145
Refresh the Cache 146

Chapter 8: Managing Global Configurations 147

Logging In as a Global Administrator 148
Logging Out of Administration Console 149
Security Recommendations While Using Administration Console 149
Configuring Channels and Accounts Associations 149
Configuring RiskMinder Properties 151
Configuring RiskMinder Properties at the System Level 153
Enabling the RiskMinder Model 155
Managing Global Rule Configurations 156
Configuring Rulesets 157
Understanding RiskMinder Scoring 159
Configuring the RiskMinder Predictive Model 160
Configuring Out-of-the-Box Rules 162
Adding New Rules 163
Deploying a New Rule 183
Deploying a New Rule Without Scoring 185
Deploying New Device-Based Rules 187

Editing Rule Definitions Using the Rule Builder 191
Deleting a Rule 201
Uploading Rule List Data 202

Chapter 9: Configuring Callouts 217

Understanding Callouts 218
Callout Implementation 219
Types of Callouts 220
Configuring Callouts 222
Configuring Evaluation Callout 223
Configuring Scoring Callout 225
Working with the Sample Callout 227
Deploying Sample Callouts 228
Configuring RiskMinder Server to Communicate With Sample Callouts 229

Chapter 10: Managing Organizations 231

Creating and Activating Organizations 232
Creating Organizations in RiskMinder Repository 232
Creating Organizations in LDAP Repository 236
Searching for Organizations 243
Updating Organization Information 244
Updating the Basic Organization Information 245
Updating RiskMinder-Specific Configurations 247
Uploading Users and User Accounts in Bulk 248
Viewing the Status of the Bulk Data Upload Request 252
Refreshing Organization Cache 253
Deactivating Organizations 254
Activating Organizations 255
Activating Organizations in Initial State 256
Deleting Organizations 257

Chapter 11: Managing Organization-Specific RiskMinder Configurations 259

Accessing Organization-Specific RiskMinder Configurations 260
Creating Rulesets 261
Assigning Rulesets 261
Deleting Rulesets 262
Using Global Rule Configurations 263
Configuring RiskMinder for an Organization 263

Chapter 12: Managing Administrators 265

Creating Administrators 266
Changing Profile Information for Administrators 268
Searching Administrators 269
Updating Administrator Information 270
Changing Administrator Role to User 271
Configuring Account IDs for Administrators 272
    Creating Account IDs 273
    Updating Account IDs 274
    Deleting Account IDs 274
Deactivating Administrators 275
Deactivating Administrators Temporarily 276
Activating Administrators 277
Deleting Administrators 278

Chapter 13: Managing Users 279

Creating Users 279
Searching Users 281
Updating User Information 282
Promoting Users to Administrators 284
Configuring Account IDs for Users 285
    Creating Account IDs 286
    Updating Account IDs 287
    Deleting Account IDs 287
Deactivating Users 288
Deactivating Users Temporarily 289
Activating Users 290
Deleting Users 291

Chapter 14: Tools for System Administrators 293

DBUtil: RiskMinder Database Tool 294
    Using DBUtil Options 294
    Updating the Master Key 297
arrfversion: RiskMinder Modules Version Display Tool 299
arrfclient: Server Refresh and Shutdown Tool 299
    Before You Use the Tool 300
    Running the Tool in Interactive Mode 301
arrfserver: RiskMinder Server Tool 302
    Running the Tool in Interactive Mode 302
arrfupload: Quova Data Upload Tool 303

Before You Use the Tool 304
Using the Tool 305

Chapter 15: Managing Cases 309

Understanding RiskMinder Cases 310
Case Basics 311
Case Management Components 312
Case Roles 318
Customer Service Representatives 318
Queue Managers 320
Fraud Analysts 321
Case Role Privilege Summary 321
Case States 322
New 322
Open 322
In Progress 323
On Hold 323
Expired 323
Closed 324
Case Management Workflows 324
Case Generation 325
Case Queuing 325
Case Assignment 326
Case Handling 327
Case Expiry 327
Fraud Analysis 328
Creating a New Queue 329
Managing the Case Queue 330
Viewing the Status of the Queue 331
Updating the Status of the Queue 332
Disabling the Queue 333
Enabling the Queue 334
Deleting the Queue 335
Rebuilding a Queue 336
Handling Cases 337
Working on Cases (CSRs) 337
Managing Inbound Customer Calls (CSRs) 341
Generating Case Management Reports 342
Case Activity Report 342
Average Case Life Report 343
Generating a Case Management Report 345

Chapter 16: Managing Reports 347

Summary of Reports Available to Administrators 347
Administrator Reports 350
My Activity Report 351
Administrator Activity Report 352
User Activity Report 353
User Creation Report 354
Organization Report 355
RiskMinder Reports 356
Instance Management Report 357
Analyzing Transactions 358
Risk Evaluation Detail Activity Report 369
Risk Advice Summary Report 372
Fraud Statistics Report 373
Rule Effectiveness Report 374
False Positives Report 374
Device Summary Report 375
Exception User Report 376
Rule Configurations Report 376
Rules Data Report 377
Case Management Reports 377
Generating Reports 378
Notes for Generating Reports 378
Generating Reports 379
Exporting Reports 380
arreporttool: Report Download Tool 380

Appendix A: RiskMinder Rule Tags 385

Appendix B: RiskMinder Logging 389

About the Log Files 390
Installation Log File 391
Startup Log Files 391
Transaction Log Files 394
Administration Console Log File 396
UDS Log File 397
Format of RiskMinder Server and Case Management Server Log Files 398
Format of the UDS and Administration Console Log Files 399
Supported Severity Levels 399
Server Log File Severity Levels 400

Administration Console and UDS Log File Severity Levels 400
Sample Entries for Each Log Level 402

Appendix C: Geolocation and Anonymizer Data 405

Understanding Geolocation and Anonymizer Data 406
Using Geolocation Data in RiskMinder Rules 406
Negative Country Check 407
Zone Hopping Check 407
IP Routing Type 407
Connection Type 408
Line Speed 409
Region 410
Continent 410
Using Anonymizer Data 411
Using the Negative IP Address List 411

Appendix D: Summary of Server Refresh and Restart Tasks 413

Appendix E: Multi-Byte Character and Encrypted Parameters 415

Appendix F: Currency Conversion 419

Understanding Currency Conversion 420
Currency Conversion Table 421
Guidelines for Using the ARRFCURRCONVRATES Table 422

Appendix G: Troubleshooting RiskMinder Errors 423

Administration Console Errors 424
User Data Service Errors 428

Chapter 1: Overview of the Administration Console

The Administration Console is a Web-based, operation and system management tool, which provides a consistent, unified interface for managing CA RiskMinder.

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

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

- About the Administration Console (see page 14)
- Elements of the Administration Console (see page 15)
- Supported Roles (see page 16)
- Next Steps: Quick Administration (see page 23)

Note: CA RiskMinder still contains the terms Arcot and RiskFort in some of its code objects and other artifacts. Therefore, you will find occurrences of Arcot and RiskFort in all CA RiskMinder documentation. In addition, some of the topics in this guide do not follow the standard formatting guidelines. These inconsistencies will be fixed in a future release.

About the Administration Console

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

You can use the Administration Console to configure RiskMinder Server, create users, assign administrative roles, and complete other administrative operations and configuration tasks, such as:

- Configure communication parameters between the server and other RiskMinder components
- Configure RiskMinder rules according to your business requirements
- Manage organizations, administrators, and users
- Generate administration, transaction, case management, and configuration reports

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

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

Elements of the Administration Console

A typical Administrative screen can be divided into the following elements:

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

The following table describes these elements.

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

Console Messages

All the information, warning, and error messages that are generated in the course of using the Administration Console are displayed under the Title area of the body page.

While the error messages are displayed in red, the messages indicating success are displayed in blue. Any additional instructions are also a part of these messages.

Supported Roles

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

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

The Administration Console supports the following types of roles:

- Users (see page 16)
- Default Administrative Roles (see page 17)
- Custom Roles (see page 23)

Users

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

If the user already exists in your LDAP system, then you need to map the LDAP attributes to attributes supported by RiskMinder database. See "Creating Organizations in LDAP Repository" (see page 236) for more information on how to do this.

To enroll users in the RiskMinder database, select the organization whose repository type is Arcot Database. See "Creating Organizations in RiskMinder Repository" (see page 232) for more information on how to do this.

Default Administrative Roles

The Administration Console is shipped with an out-of-the-box administrative user called the Master Administrator (see page 20) who can perform high-level configurations. Other than this role, you must assign users to administrative roles to administer the RiskMinder system or to access your business data. An administrative role typically comprises a set of privileges based on a job function profile and the scope in which these permissions are applicable. The users with administrative privileges are referred to as *administrative users*.

Note: See "Summary of Administrative Privileges" (see page 59) for a comprehensive list of privileges available.

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

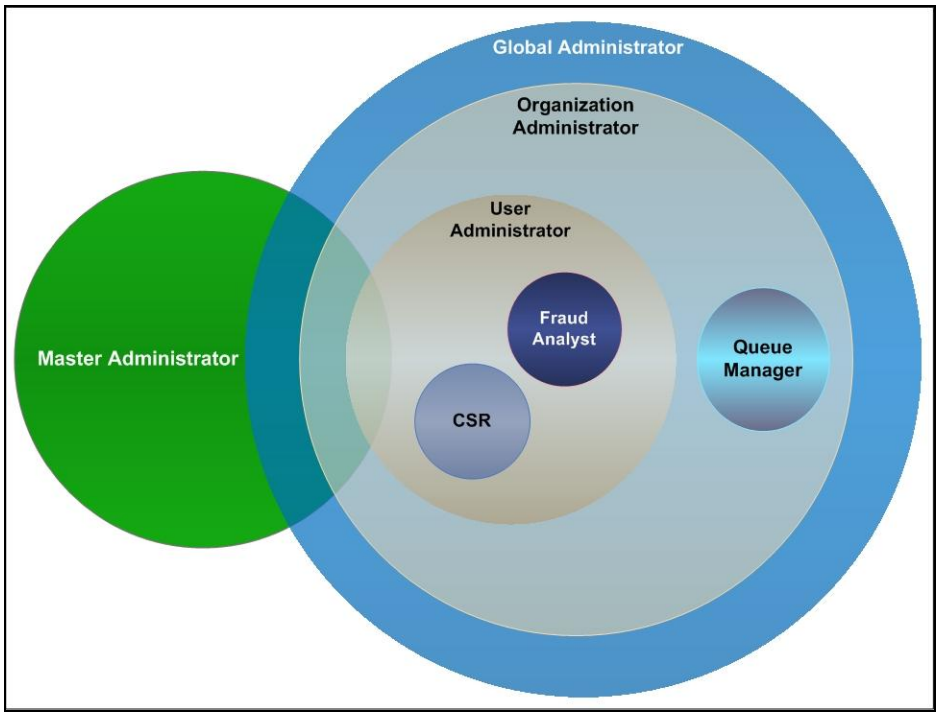
- Master Administrator (see page 20)
- Global Administrator (see page 21)
- Organization Administrator (see page 22)
- User Administrator (see page 22)

In addition, you can also create Custom Roles (see page 23). RiskMinder is shipped with three pre-defined custom roles that are required for Case Management:

- Queue Manager
- Customer Support Representative
- Fraud Analyst

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

The following figure depicts these administrative roles and the relationships between the privileges available to these roles. The topics following the figure discuss the supported administrator levels in details.



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

Scope of an Administrative Role

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

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

Important Notes About Scope

While creating an administrative role, you must remember that:

- The scope of the Master Administrator (see page 20) is **All Organizations**, and this administrator manages *all* existing and other organizations that will be created in the future.
- A role (Global Administrator (see page 21), Organization Administrator (see page 22), or User Administrator (see page 22)) can manage their peers and the roles with lesser privileges, provided they have scope on the organization to which the administrators belong to.

  For example, a Global Administrator can manage other Global Administrators, Organization Administrators and User Administrators. However, they *cannot* manage a Master Administrator.
- The scope of a Global Administrator (see page 21) role *can* be defined as All Organizations, in which case the administrator can manage all existing as well as future organizations.
- An Organization Administrator (see page 22) or a User Administrator (see page 22) role can be limited to manage only specific organizations.

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

Master Administrator

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

The primary responsibilities of an MA are to:

- Bootstrap (or initialize) the system after installation.
- Configure the User Data Service (UDS) connection parameters.
- Configure the global settings for organizations and cache refresh settings for the Administration Console.
- Configure custom locales.
- Set the Default Organization.
- Configure attributes for encryption.
- Configure account types and email and telephone types.
- Enable authentication and authorization for Web services.
- Configure the RiskMinder Server communication parameters.
- Configure and manage RiskMinder Server and Case Management Queuing Server instances.
- Configure the RiskMinder Server protocol settings.
- Configure the authentication mechanism for the Administration Console, Server components, and other miscellaneous settings.
- Create and manage organizations, if required.
- Create and manage administrators of any role (Global, Organization, or User Administrator), as required.
- Manage Custom Roles (see page 23).

At the end of a successful deployment of Administration Console, you must log in for the first time as an MA. A default password (master1234!) is assigned to the MA account (masteradmin). Because the actions of an MA can affect the security of the entire system, it is recommended that you change this password after you log in to the Console for the first time. It is also recommended that you safeguard this password and change it regularly.

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

Resetting the Master Administrator Password

If your MA account password is locked because of multiple failed password attempts, you can run the **arcot-masteradmin-password-reset-2.0.sql** script to reset your password. This script is available in the **<INSTALL_HOME>\dbscripts\<database>** folder.

After running the script, you need to log in with the default password (**master1234!**), and then reset the password.

Global Administrator

The Global Administrator (GA) is the second level in the administrative hierarchy. These administrators can perform most of the tasks of an MA, except for the following:

- Bootstrapping the system
- Performing initial Administration Console configurations
- Setting the Default Organization
- Configuring custom locales
- Enabling authentication and authorization for Web services
- Configuring global attribute encryption set
- Configuring global email and telephone types
- Specifying server configurations
- Managing custom roles

The main tasks of a GA are to:

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

  Note: This includes editing the organization details.
- Create and manage users, as required.
- Configure global rules and scoring.
- Assign configurations.
- Configure Callouts.

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

Organization Administrator

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

The main tasks of an OA are to:

- Create and manage other Organization or User Administrators, as required.
- Create and manage the users that belong to the organizations in their purview.
- Manage organizations in their purview.
- Refresh the cache of organizations in their purview.
- Configure the authentication policy for the organization.
- Manage (update) organization-specific configurations.

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

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

User Administrator

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

- Create and manage users.
- Manage end user cases.

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

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

Custom Roles

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

- Global Administrator (see page 21)
- Organization Administrator (see page 22)
- User Administrator (see page 22)

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

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

In addition to the custom roles that you can create, RiskMinder is also shipped with three pre-defined custom roles that are required for Case Management. These roles include:

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

See Working with Custom Roles (see page 55) for more information on working with these custom roles. See Managing Cases (see page 309) for more information on Case Management roles.

Next Steps: Quick Administration

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

- For Simple Deployments (see page 24)
- For Complex Deployments (see page 26)

For Simple Deployments

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

Note: See "Planning the Deployment" in the *CA RiskMinder Installation and Deployment Guide* for more information on this type of deployments.

The following table summarizes the typical characteristics of this deployment type.

Characteristic	**Details**
Deployment Type	■ Development, proof of concept, initial testing, or initial pilot ■ Small to medium businesses (SMBs) ■ Regional deployment within an enterprise
Geographic Expanse	Typically restricted to a single location
Deployment Requirements	Ease of implementation and management

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

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

1. Ensure that RiskMinder is installed and configured properly and that you have deployed the WAR files for the Administration Console.

   Note: See "Deploying RiskMinder on a Single System" in the *CA RiskMinder Installation and Deployment Guide* for more information on installing RiskMinder, deploying the WAR files, and performing other post-installation tasks.

2. Log in to the Administration Console as MA (see "Accessing the Administration Console" (see page 30)) and follow the steps in the Bootstrap wizard to initialize the system.

   Note: See "Bootstrapping the System" in the *CA RiskMinder Installation and Deployment Guide* for more information.

3. Create the required GA and UA accounts.

   See "Creating Administrators" (see page 266) for more information.

4. As a GA, configure the required RiskMinder rules to meet your business requirements.

   See "Managing Global Configurations" (see page 147) for more information.

5. Create users in RiskMinder.

   See "Creating Users" (see page 279) for more information.

With this, your system is set for risk evaluation. You can now manage the system ("Managing RiskMinder Server Instances" (see page 65)), administrators ("Managing Administrators" (see page 265)), and users ("Managing Users" (see page 279)).

For Complex Deployments

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

Note: See "Planning the Deployment" in the *CA RiskMinder Installation and Deployment Guide* for more information on this type of deployments.

The following table summarizes the typical characteristics of this deployment type.

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

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

1. Ensure that RiskMinder is installed and configured properly and that you have deployed the WAR files for the Administration Console.

   Note: See "Deploying RiskMinder on a Distributed System" in the *CA RiskMinder Installation and Deployment Guide* for more information on installing RiskMinder, deploying the WAR files, and performing other post-installation tasks in a distributed environment.

2. Log in to the Administration Console as MA (see "Accessing the Administration Console" (see page 30)) and follow the steps in the Bootstrap wizard to initialize the system.

   Note: See "Bootstrapping the System" in the *CA RiskMinder Installation and Deployment Guide* for more information.

3. Configure the Administration Console settings, which include UDS settings, global organization settings, Administration Console cache settings, and the basic username-password authentication policy for logging in to the Console.

   See "Configuring Administration Console Settings" (see page 32) for more information.

4. Set up RiskMinder Server instances on different systems.

   See "Managing RiskMinder Server Instances" (see page 65) for more information.

5. Configure the protocols that Administration Console, SDKs, and Web Services use to communicate to RiskMinder Server.

   See "Configuring Communication Protocols" (see page 72) for more information.

6. Plan and create organizations. The organization architecture is flat and each organization that you create can map to a business unit in your enterprise.

   See "Creating and Activating Organizations" (see page 232) for more information.

7. Plan and create the administrators (see "Creating Administrators" (see page 266)) and custom roles (see "Working with Custom Roles" (see page 55)), if required.

8. Create appropriate rules and rulesets to meet your business requirements, and assign these configurations.

   See "Managing Global Configurations" (see page 147) for more information.

9. Create users in RiskMinder.

   See "Creating Users" (see page 279) for more information.

10. If required, configure Secure Sockets Layer (SSL)-based communication between RiskMinder Server and its clients.

    See "Creating Trust Stores" (see page 71) for more information.

11. If you are planning to extend the RiskMinder functionality by the use of callouts, then define and configure the required configurations.

See "Configuring Callouts" (see page 217) for more information.

With this, your system is set for risk evaluation. You can now manage the system ("Managing RiskMinder Server Instances" (see page 65)), administrators ("Managing Administrators" (see page 265)), and users ("Managing Users" (see page 279)).

Chapter 2: Getting Started

This topic walks you through the steps for logging in to Administration Console as Master Administrator (see page 20) and configuring basic information, *after* you have successfully installed RiskMinder and have deployed the Console and bootstrapped it.

Note: See the *CA RiskMinder Installation and Deployment Guide* for detailed information on installing RiskMinder, deploying Administration Console, and bootstrapping it.

This topic covers:

- Accessing the Administration Console (see page 30)
- Changing Password and Profile Information (see page 31)
- Configuring Administration Console Settings (see page 32)

Accessing the Administration Console

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

- **User Name:** masteradmin
- **Password:** <*password set during bootstrap*>

To log in to Administration Console:

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

   http://<hostname>:CA Portal/arcotadmin/masteradminlogin.htm

   In the preceding URL:

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

   The Master Administrator Login page appears.
3. In the **Password** field, enter the password that you set during bootstrap, and click **Log In.**

   The landing page of Administration Console appears.

Security Recommendations While Using Administration Console

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

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

Logging Out of Administration Console

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

Changing Password and Profile Information

It is recommended that you change your Master Administrator password regularly to maintain high security, so that unauthorized persons do not gain access to Administration Console by using the MA credentials.

Use the My Profile page to change your current password and your preferences that will be reflected by default for all administrator-related and user-related tasks that you perform in future.

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

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

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

      This organization will be selected by default in the "Organization" field for all administrator-related and user-related tasks that you perform from now on. For example, when you search the administrators, by default they will be searched in the preferred organization.
   b. The Preferred Organization that will be selected by default in the "Organization" field from now on.
   c. The preferred Date Time Format.

      This Date Time Format will be shown from now on in all date-related fields, except the report criteria page, user deactivate dialog box, and the administrator credential lock section where you need to provide the date input.
   d. The preferred Locale for your login of Administration Console.

      See "Configuring Custom Locales" (see page 43) for more information on how to configure locales. The default locale is English (United States).
   e. The preferred Time Zone.

      This Time Zone will be shown from now on in all the date-related fields in Administration Console.

      The default Time Zone is GMT.
5. Click Save.

Configuring Administration Console Settings

Before you configure the RiskMinder-specific settings, it is recommended that you configure the global configurations for Administration Console. This includes the following:

- Updating UDS Configurations (see page 32)
- Refreshing the Cache (C3_RC_H2) (see page 37)
- Viewing the Status of Cache Refresh Requests (see page 39)
- Configuring Attribute Encryption (see page 41)
- Configuring Custom Locales (see page 43)
- Setting the Default Organization (see page 44)
- Configuring the Account Type (see page 45)
- Configuring Email and Telephone Type (see page 48)
- Specifying Basic Authentication Policy Settings (see page 49)
- Specifying Master Administrator Authentication Policy Settings (see page 51)
- Configuring Web Services Authentication and Authorization (see page 53)

The following topics walk you through the steps for configuring these global settings.

Updating UDS Configurations

User Data Service (UDS) is a user virtualization layer that enables access to the third-party data repositories (such as LDAP directory servers) that are already deployed by your organization. UDS enables RiskMinder Server and Administration Console to seamlessly access your existing data and leverage end-user information, without having to duplicate it in the standard RiskMinder SQL database tables.

RiskMinder can access user data either from a relational database (RDBMS) or directly from an LDAP server:

- **If you are using a relational database,** then you just need to seed the database with RiskMinder schema as a part of the post-installation configurations.
- **If you are using an LDAP directory server** and you want RiskMinder Server and Administration Console to seamlessly access it, then you must deploy User Data Service as a part of the post-installation configurations.

Updating the UDS Connectivity Configuration

To update the default UDS connectivity settings, you must use the UDS Connectivity Configuration page.

To update UDS connectivity configuration:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **System Configuration** section on the side-bar menu, click the **UDS Connectivity Configuration** link to display the page.
5. Specify the parameters, explained in the following table, on the page. All the enabled parameters on this page are mandatory.

Parameter	Default Value	Description
Protocol	TCP	The protocol to connect to the UDS service by using Administration Console. The available options are: ■ **TCP:** If you want to implement unencrypted information exchange between UDS and Administration Console, RiskMinder Server, and the RiskMinder Database. ■ **One-Way SSL:** If you want to implement SSL communication between UDS and RiskMinder components, and RiskMinder components must present their certificates when accessing UDS. ■ **Two-Way SSL:** If you want to implement SSL communication between UDS and RiskMinder components, and both UDS and RiskMinder components must present their certificates during information exchange.
Host	localhost	The IP address or host name where the UDS service is available.
Port	8080	The port at which the UDS service is available.
Application Context Root	arcotuds	The application context that is specified when UDS is deployed on the application server.
Connection Timeout (in milliseconds)	30000	Maximum time in milliseconds before the UDS service is considered unreachable.

Parameter	Default Value	Description
Read Timeout (in milliseconds)	10000	The maximum time in milliseconds to wait for a response from UDS.
Idle Timeout (in milliseconds)	30000	The time (in milliseconds) after which an idle connection not serving requests will be closed.
Server Root Certificate		The path to the Certificate Authority (CA) certificate file of the UDS server. The file must be in PEM format. **Note:** This field will *not* be enabled if you selected the **TCP** option in the Protocol field.
Client Certificate		The path to the CA certificate file of Administration Console. The file must be in PEM format. **Note:** This field will *not* be enabled if you selected the **TCP** or **One-Way SSL** option in the Protocol field.
Client Private Key		The location of the file that contains the CA's private key. The path can be an absolute path or relative to ARCOT_HOME. **Note:** This field will *not* be enabled if you selected the **TCP** or **One-Way SSL** option in the Protocol field.
Minimum Connections	4	The minimum number of connections that will be created between RiskMinder Server and the UDS server.
Maximum Connections	32	The maximum number of connections that can be created between RiskMinder Server and the UDS server.

1. Click **Save** to save the changes you made.
2. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Updating UDS Parameters

If you need to update the UDS parameters, you must use the UDS Configuration page.

To update the UDS parameters:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **UDS Configuration** section on the side-bar menu, click the **UDS Configuration** link to display the page.
5. Specify the parameters, explained in the following table, on the page.

Parameter	Default Value	Description
Search Configuration		
Maximum Search Return Count	500	The maximum number of records that will be returned for all **Search** operations in Administration Console.
LDAP Configuration **Note:** These fields cannot be edited using Administration Console. For information on configuring these parameters, see the *CA RiskMinder Installation and Deployment Guide*.		
LDAP Connection Pool Initial Size	NA	The initial number of connections between UDS and LDAP that will be created in the pool.
LDAP Connection Pool Maximum Size	NA	The maximum number of connections allowed between UDS and LDAP.
LDAP Connection Pool Preferred Size	NA	The preferred number of connections between UDS and LDAP.
LDAP Connection Pool Timeout (in milliseconds)	NA	The period for which UDS waits for a response from LDAP, when a new connection is requested.
Authentication and Authorization Token Validity Configuration		
Purge Interval (in seconds)	3600	The maximum interval after which an authentication token is purged from the database, *after* the token expires.
Validity Period (in seconds)	86400	The maximum period (default is one day) after which an issued authentication token expires.

6. Click **Save** to save the changes you made.
7. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Refreshing the Cache

Administration Console caches certain data, which serves frequently-accessed Console pages and UDS data faster. Typically, organizations and roles are cached. RiskMinder maintains cached data at the system level and at the organization level.

Data Cached at the System Level

The following data is cached at the system level:

- All system-level configurations
  - UDS configuration and UDS connectivity
  - LDAP connection pool details
  - List of organizations
  - Global key label
  - Account type details
  - Custom roles
- Global data
  - Encryption sets
  - Localization configuration
  - Email and Telephone types
  - Authentication and Authorization configuration
- Resources applicable to all organizations

  Global account types that are applicable to all organizations

Data Cached at the Organization Level

The following data is cached at the organization level:

- Data that is applicable to individual organizations

  Configurations that do not refer to global data, such as encryption set, localization configuration, and email and telephone types
- Resources applicable to a set of organizations

  Organization-specific account types
- Rules

Important! When you make data configuration changes that involve both system-level and organization-level changes, the system cache is refreshed first, followed by the organization cache. Any change in this order of cache refresh may result in inconsistent behavior.

Cache Refresh Order Example

Account type details and global account types are cached at the system level. Whenever you create a new account type, irrespective of whether it is global or organization-specific, you must refresh the system cache. In addition, if the account type is organization-specific, you must refresh the cache of all the organizations involved in the scope. For more information on account types, see "Configuring the Account Type" (see page 45).

Refreshing the Cache

If you have made any configuration changes, you must refresh the cache of the affected server instances for the changes to take effect. RiskMinder now provides an *Integrated Cache Refresh* feature that enables administrators to refresh the cache of all server instances from Administration Console.

Note: The Master Administrator (MA) and Global Administrator (GA) can refresh the cache of Administration Console and all instances of RiskMinder Server and Case Management Queuing Server. The MA, GA, and Organization Administrator (OA) can refresh the cache of the organizations within their scope.

To refresh the cache:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the System Configuration section on the side-bar menu, click the Refresh Cache link to display the page.
5. Select one or both of the following:
   - Select Refresh System Configuration to refresh the cache configuration of Administration Console, User Data Service, and all RiskMinder Server and Case Management Queuing Server instances.
   - Select Refresh Organization Configuration to refresh the cache configuration of all organizations in your purview.
6. Click OK.
7. Click OK in the confirmation dialog box that appears.

   A message with a Request ID for the current cache refresh request is displayed.

Viewing the Status of Cache Refresh Requests

To view the status of your cache refresh request:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the System Configuration section on the side-bar menu, click the Check Cache Refresh Status link to display the page.
5. Enter a Request ID or select a Status and click Search to check the status of the cache refresh request.

   The cache refresh details are displayed. You can see the status of the cache refresh operation for the different server instances.

   The search result lists the following:

   - The unique identifier of the cache refresh request
   - Organizations that were affected by cache refresh request
   - Time when the request was received
   - The event type
   - RiskMinder Server instances (see the following table) that were affected by cache refresh request

Parameter	Description
Resource	The RiskMinder resource that was refreshed. Possible values are: ■ **AdminConsole** For Administration Console and User Data Service ■ **RiskFort** For RiskMinder Server
Server Instance ID	Specifies the unique identifier of the server instance that was refreshed. ■ For Administration Console and User Data Server, this value is fetched from the InstanceID parameter set in arcotcommon.ini file. ■ For RiskMinder Server, it is the instance name of RiskMinder Server. By default, it is a combination of host name and a unique identifier.

Parameter	Description
Server Instance Name	Specifies the instance name of the RiskMinder component that was refreshed. Possible values are: ■ Administration Console ■ User Data Service ■ Instance name of RiskMinder Server
Host Name	Specifies the name of the system on which the refreshed component is installed.
Status	Specifies the status of the cache refresh request.

Configuring Attribute Encryption

By default, RiskMinder stores the user-related data in plain format in the database tables that you seed during installation. To encrypt this data, you need to use the Attribute Encryption Set Configuration page and select the user attributes that you want to encrypt. See appendix, "Multi-Byte Character and Encrypted Parameters" (see page 415) for the list of attributes that can be stored in an encrypted format.

To configure attribute encryption and data masking:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the System Configuration section on the side-bar menu, click the Attribute Encryption Configuration link to display the page.

   Note: If you choose to encrypt the User Identifier attribute, all the following attributes that help in uniquely identifying the user are also encrypted:
   – User ID
   \xE2\x80\x93 Account ID
   – Account ID attributes
5. In the Select Attribute(s) for Encryption section, select the attributes that you want to encrypt from the Available Attributes for encryption list to the Attributes Selected for encryption list.

   Click the > or < buttons to move selected attributes to the desired list. You can also click the >> or << buttons to move all attributes to the desired lists.
6. In the Data Masking Configuration section, specify the parameters described in the following table.

   Note: Data masking is the process of hiding specific elements within the actual data string. It ensures that sensitive data is replaced with some data other than the real one.

Parameter	Description
Type	Select an option from the drop-down list to Mask or Unmask the attributes configured for encryption.
Start Length	The number of characters to be masked or unmasked from the start of the actual data string.
End Length	The number of characters to be masked or unmasked from the end of the actual data string.
Masking Character	The character that will be used to mask (hide) the actual data.

7. Click **Save** to save your changes.
8. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Examples of Masking and Unmasking

If you want to mask a user name that has been configured for encryption, and the **Start Length**, **End Length**, and **Masking Character** are 2, 2, and x, then the user name "mparker" is masked as "xxarkxx".

If you want to unmask a user name that has been configured for encryption, and the **Start Length**, **End Length**, and **Masking Character** are 2, 2, and x, then the user name "mparker" is unmasked as "mpxxxer".

Configuring Custom Locales

RiskMinder supports *localization*, which is the process of adapting internationalized software for a region or language of your choice, by adding locale-specific components and translating the text. You can use the Localization Configuration page in Administration Console to configure the locales that RiskMinder supports.

Before you configure the available locales, you can add additional locales that will appear in the Available list for you to choose. See the topic titled "Preparing for Localization" in the *CA RiskMinder Installation and Deployment Guide*.

To configure custom locales and set the default locale and date time format:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the System Configuration section on the side-bar menu, click the Localization Configuration link to display the page.
5. In the Configure Supported Locales section, select the locales that you want to add from the Available list, and use the > or < buttons to move them to the Selected list.

   You can also click the >> or << buttons to move all locales to the desired lists.
6. In the Configure Default Locale section, select the Default Locale from the drop-down list.
7. In the Configure Default Date Time Format section, specify the Date Time Format you want to use.

   Move your cursor over the question mark icon to determine the Date Time Format you want to use.

   Note: The Administrator can change the Locale and Date Time Format at the organization level and also on the My Profile page.
8. Click Save to save your changes.
9. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Setting the Default Organization

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

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

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

To specify the Default Organization:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the UDS Configuration section on the side-bar menu, click the Set Default Organization link to display the page.
5. Under Default Organization, select the organization that you want to set as the Default Organization from the Organization Name list.
6. Click Save to save the changes you made on this page.
7. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring the Account Type

All RiskMinder users are identified in the system by a unique user name. RiskMinder supports the concept of an *account* or *account ID*, which is an alternate ID to identify the user in addition to the user name. A user can have none or one or more accounts or account IDs.

For example, consider a banking institution that uses the ID from the Customer Information File (CIF), to identify the customer Robert Laurie. In addition, Robert uses his account number to transact with the bank for his fixed deposits and a different account ID for online banking. So, Robert has the following account IDs:

- User name: BNG02132457678
- Account ID for fixed deposits: 000203876544
- Account ID for online banking: rlaurie

An *account type* is an attribute that qualifies the account ID and provides additional context about the usage of the account ID. An account ID uniquely identifies a user for the given account type.

For example, you can create an account type called FIXED_DEPOSITS for the 000203876544 account ID, and another account type called ONLINE_BANKING for the account ID rlaurie.

Now, Robert can log in to the system and can be identified by using any of the following:

- BNG02132457678
- FIXED_DEPOSITS/000203876544
- ONLINE_BANKING/rlaurie

You must first create an account type in Administration Console before you can create account IDs. You can configure the account type to be available to specific organizations only or to all organizations, including those that will be created in the future. At the organization level, each organization can choose to support a set of account types.

Note: No two users in a given organization can have the same account ID for an account type. At any given point of time, the following combinations are unique:
– Organization name, account type, and account ID
– Organization name, user name

Creating a New Account Type

To create a new account type:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.

4. Under the UDS Configuration section on the side-bar menu, click the Configure Account Type link to display the page.
5. (If this is the first account type you are adding) In the Add New Account Type section:
   a. Enter the Name of the account type.
   b. Enter a Display Name for the account type.
   c. If required, expand the Custom Attributes section by clicking the + sign and specify the Name and Value of any custom attributes that you want to add for this account type.
6. In the Assign to Organizations section:
   - Select Apply to all Organizations if you want to use this account type for all existing organizations and any organizations that might be created in future.

     Note: Such accounts appear under Global Accounts on the Configure Account Type page at the organization level.

     or

   - Select the organization to which you want to assign the account type from the Available list and move it to the Selected list.

     Note: The accounts assigned to specific organizations appear under **Organization-Specific Accounts** on the Configure Account Type page at the organization level.

     Click the > or < buttons to move selected organizations to the desired list. You can also click the >> or << buttons to move all organizations to the desired lists.
7. Click Create to create the account type.
8. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Updating an Account Type

To update an existing account type:

1. Select the account type from the Select Account Type drop-down list.
2. Modify the required fields, and click Update.

   Note: Once you have created an account type, you cannot change the Name of the account type.
3. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Deleting an Account Type

To delete an existing account type:

1. Select the account type from the Select Account Type drop-down list.
2. Click Delete.

   Important! You cannot delete an account type if you have created user accounts for that type.
3. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring Email and Telephone Type

RiskMinder allows you to specify multiple email addresses and telephone numbers while creating users and administrators. The MA can configure multiple email and telephone types at the global level, which automatically become available to all organizations. The MA can also specify certain email and telephone types as mandatory and others as optional. When you create users and administrators in an organization, you will be prompted to enter values for the email and telephone types that the MA has configured. You can choose to override the global configuration by configuring different email and telephone types while creating organizations.

Note: Email and telephone type attributes configured at the organization level take precedence over the values configured at the global level.

Email and Telephone Type Example

Assume that the MA has configured the following email and telephone types that all organizations must use:

- (Mandatory) Email type: Work Email
- (Optional) Email type: Personal Email
- (Mandatory) Telephone type: Work Phone
- (Optional) Telephone type: Home Phone

Now, when a GA creates an administrator for an organization *Org1* that uses the global configuration, the GA *must* provide values for Work Email and Work Phone. The GA can add additional email and telephone types, if required, but cannot delete the global configurations for email and telephone types.

To configure the email and telephone type attributes:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the UDS Configuration section on the side-bar menu, click the Email/Telephone Type Configuration link to display the page.
5. In the Configure Email Type section, specify:
    - Priority of the Email Type if more than one Email Type has been configured. Use the up and down icons to change the priority. Priority defines the order in which Email Types are displayed on the screen when multiple Email Types have been configured.
    - Type of email that you want to configure, for example, work or personal.
    - Display Name of the Email Type.
    - Whether the Email Type is Mandatory.

For example, you can configure work email with a higher priority than your personal email so that work email gets displayed first.

6. In the Configure Telephone Type section, specify:
   - Priority of the Telephone Type if more than one Telephone Type has been configured. Use the up and down icons to change the priority. Priority defines the order in which Telephone Types are displayed on the screen when multiple Telephone Types have been configured.
   - Type of phone number that you want to configure, for example, home or work.
   - Display Name of the Telephone Type.
   - Whether the Telephone Type is Mandatory.

   Note: You can add multiple Email and Telephone types by clicking the **+** icon.
7. Click Save to save your changes.
8. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Specifying Basic Authentication Policy Settings

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

- If you select the **Basic User Password** option while creating an organization, then you can use the default authentication policy, as discussed in "Configuring the Basic Authentication Password Policy" (see page 50) (for global level).
- If you select the **LDAP User Password** option, the password stored in LDAP is used by the administrator to log in. The authentication policy is defined in the LDAP system.
- If you select the **WebFort User Password** option, then ensure that AuthMinder is deployed and accessible.

Note: See the *CA AuthMinder Installation and Deployment Guide* and the *CA AuthMinder Administration Guide* for detailed information to install and configure AuthMinder in your environment.

Configuring the Basic Authentication Password Policy

As the name implies, *Basic Authentication* method enables administrators to log in to the Console by using a user ID and the corresponding password.

You can use the Basic Authentication Policy page to strengthen the password policy by enforcing restrictions, such as password length, allowed number of special characters, and the number of failed login attempts allowed before locking the account.

To configure the Basic Authentication policy:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the Authentication section on the side-bar menu, click the Basic Authentication Policy link to display the corresponding page.
5. Specify the parameters explained in following table in the Password Policy Configuration section. All the parameters on this page are mandatory.

Parameter	**Default Value**	**Description**
Minimum Password Length	6	The minimum number of characters that the password must contain. You can set a value between 6 and 32 characters.
Maximum Password Length	25	The maximum number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password must contain. You can set a value between 0 and 32 characters.
Maximum Password History Count	3	The maximum number of previously used passwords that cannot be reused.
Validity Period	180 days	The maximum number of days for which a password is valid.
Allow Multi-Byte Characters The following options are disabled if you select this check box.		Select this option if you want to allow multi-byte characters in the password.

Parameter	Default Value	Description
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of Allowed Special Characters that the password must contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#$%^&*()_+	The list of special characters that the password can contain.

6. Click **Save** to save the changes you made on this page.
7. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Specifying Master Administrator Authentication Policy Settings

By default, the Master Administrator follows the *Basic Authentication* method that enables them to log in to the Console by using a user ID and the corresponding password.

You can use the Master Administrator Authentication Policy page to strengthen the MA's password policy by enforcing restrictions, such as password length, allowed number of special characters, and the number of failed login attempts allowed before locking the account.

To configure the Master Administrator Authentication policy:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **Authentication** section on the side-bar menu, click the **Master Administrator Authentication Policy** link to display the corresponding page.
5. Specify the parameters explained in the following table in the **Password Policy Configuration** section. All the parameters on this page are mandatory.

Parameter	Default Value	Description
Minimum Password Length	6	The minimum number of characters that the password must contain. You can set a value between 6 and 32 characters.

Parameter	Default Value	Description
Maximum Password Length	25	The maximum number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password must contain. You can set a value between 0 and 32 characters.
Maximum Password History Count	3	The maximum number of previously used passwords that cannot be reused.
Validity Period	180 days	The maximum number of days for which a password is valid.
Allow Multi-Byte Characters The following options are disabled if you select this check box.		Select this option if you want to allow multi-byte characters in the password.
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of Allowed Special Characters that the password must contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#$%^&*()_+	The list of special characters that the password can contain.

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

Configuring Web Services Authentication and Authorization

RiskMinder provides Web services to programmatically perform the operations that are supported by Administration Console. You can secure these Web services calls by enabling authentication and authorization. You can use Administration Console to select the Web services for which you want to enable authentication and authorization.

Note: See "Managing Web Services Security" in the *CA RiskMinder Web Services Developer's Guide* for more information on how Web services authentication and authorization works.

To configure Web services authentication and authorization:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the Web Services section on the side-bar menu, click the Authentication and Authorization link to display the page.
5. In the Web Services section, select and move the Web services from the Disabled list to the Enabled list.

   Click the > or < buttons to move selected Web services to the desired list. You can also click the >> or << buttons to move all Web services to the desired lists.
6. Click Save to save your changes.
7. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Chapter 3: Working with Custom Roles

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

RiskMinder is shipped with out-of-the-box roles that are associated with pre-defined privileges. See "Supported Roles" (see page 16) for more information on this topic. However, RiskMinder also provides you the capability to manipulate these pre-defined roles if:

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

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

- Understanding Custom Roles (see page 55)
- Creating a Custom Role (see page 57)
- Updating Custom Role Information (see page 58)
- Deleting a Custom Role (see page 59)
- Summary of Administrative Privileges (see page 59)

Understanding Custom Roles

As an MA, you can create *new administrative roles* that inherit a subset of privileges from one of the following pre-defined parent roles, as discussed in "Overview of the Administration Console" (see page 13):

- Global Administrator (see page 21)
- Organization Administrator (see page 22)
- User Administrator (see page 22)

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

When you create a custom role, it becomes available as a role option when you create or update an administrator. In addition to creating custom roles, you can update and delete them.

Things That You Should Know About Custom Roles

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

  For example, you *cannot* create a custom UA role that has privileges to manage users (UA privilege) and create organizations (OA privilege.)
- You cannot assign new privileges to a custom role, if the parent role does not have these privileges.

  For example, if the pre-defined OA role does not have the privilege to create an organization, then the custom role based on this OA role cannot have that privilege either.
- When you create a custom role, a task representing one or more privileges will continue to be visible, as long as at least one of the privileges is *still* available.

  For example, the **Search Organizations** link will appear if the Update privilege is still available, even though the Activate, Deactivate, and Delete privileges are disabled.
- A new custom role is available to other instances of Administration Console *only after* you refresh the Administration Console server cache.

Pre-Defined Custom Roles

In addition to the custom roles that you can create, RiskMinder has three pre-defined custom roles that are required for Case Management. These roles include:

- **QM:** The Queue Manager role has the required privileges to supervise cases. This role is derived from the default Organization Administrator (see page 22) role.
- **CSR:** The Customer Support Representative role has the required privileges to work on cases and handle end-user calls.This role is derived from the default User Administrator (see page 22) role.
- **FA:** The Fraud Analyst role has the required privileges to analyze cases to find hidden trends and patterns. This role is also derived from the default User Administrator (see page 22) role.

See "Managing Cases" (see page 309) for detailed information on Case Management and the Queue Manager, Customer Support Representative, and Fraud Analyst roles.

You can see these out-of-the-box custom roles on the Update Custom Role page.

Creating a Custom Role

To create a custom role:

1. Ensure that you are logged in as the MA.
2. Activate the Users and Administrators tab.
3. Click the Manage Roles link on the submenu of the tab.
4. Under the Manage Roles section, click the Create Custom Role link. The Create Custom Role page appears.
5. In the Role Details section, specify the following information:
   - Role Name: The unique name to identify the new role. This name is used internally by RiskMinder by authenticating and authorizing this new role.
   - Role Display Name: The descriptive name of the role that appears on all other Administration Console pages and reports.
   - Role Description: The useful information related to the role for later reference.
   - Role Based On: The pre-existing role from which this custom role should be derived.
6. In the Set Privileges section, specify the roles that will not be available to the new role:
   a. In the Available Privileges list, select all the privileges that you need to disable for the custom role.

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

   b. Click the > button to move the selected privileges to the Unavailable Privileges list.
7. Click **Create** to create the custom role.
8. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Updating Custom Role Information

To update an existing custom role definition:

1. Ensure that you are logged in as the MA.
2. Activate the Users and Administrators tab.
3. Click the Manage Roles link on the submenu of the tab.
4. Under the Manage Roles section, click the Update Custom Role link.

   The Update Custom Role page appears.
5. Select the Role Name that you want to update.
6. In the Role Details section, change the Role Display Name and Role Description, if required.
7. In the Set Privileges section, if required, specify the list of privileges that will not be available to the role:
   a. In the Available Privileges list, select all the privileges that you need to disable for the new role.

      This list displays all the privileges available to the administrative role that you selected in the Role Based On field.
   b. Click the > button to move the selected privileges to the Unavailable Privileges list.
8. In the Set Privileges section, if required, specify the list of privileges that will be available to the role:
   a. In the Unavailable Privileges list, select the privileges that you want to enable for the new role.

      This list displays all the privileges that are not available to the administrative role that you selected in the Role Based On field.
   b. Click the < button to move the selected privileges to the Available Privileges list.
9. Click Update to update the Custom role definition.
10. Refresh all deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Deleting a Custom Role

Important! If you need to delete a custom role that is currently assigned to an administrator, then you must first change the role of all administrators who have been assigned this role by using the Update Administrator page and then follow the instructions in this topic.

To delete an existing custom role:

1. Ensure that you are logged in as the MA.
2. Activate the **Users and Administrators** tab.
3. Click the **Manage Roles** link on the submenu of the tab.
4. Under the **Manage Roles** section, click the **Delete Custom Role** link.

   The Delete Custom Role page appears.
5. In the **Role Details** section, select the custom role that you need to delete from the **Role Name** list.
6. Click **Delete** to delete the selected custom role.
7. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Summary of Administrative Privileges

The following table summarizes the privileges available to the three supported levels of administrators using which you will create a custom role.

The column name acronyms used in the table are:

- Global Administrator --> **GA**
- Organization Administrator--> **OA**
- User Administrator --> **UA**

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

Privilege	GA	OA	UA
Organization Management Privileges See "Managing Organizations" (see page 231) for more information on the tasks related to these privileges.			
Create Organization		X	X
Update Organization			X

Privilege	GA	OA	UA
Update Organization Status			X
List Organizations			
Retrieve Default Organization			
Delete Organization			X
Account Type Management Privileges See "Configuring the Account Type" (see page 45) for more information on the tasks related to these privileges.			
Create Account Type		X	X
Update Account Type			X
Delete Account Type		X	X
Administrator Management Privileges See "Managing Administrators" (see page 265) for more information on the tasks related to these privileges.			
Create Administrator			X
Update Administrator			
Delete Administrator			X
User Management Privileges See "Managing Users" (see page 279) for more information on the tasks related to these privileges.			
Create User			
Update User			
Update User Status			
List Users			
List Users for Account			
Get User Status			
Set User Custom Attributes			

Privilege	GA	OA	UA
Search Users			
Get User Details			
Get PAM			
Set PAM			
Delete User			
User Account Management Privileges			
Create User Account			
Update User Account			
List User Accounts			
Retrieve User Account			
Delete User Account			
Cache Management Privileges See "Refreshing the Cache" (see page 37) for more information on the tasks related to these privileges.			
Refresh System Cache		X	X
Refresh Organization Cache			X
View Global Cache Refresh Request		X	X
View Organizational Cache Refresh Request			X
Email and Telephone Type Privileges See "Configuring Email and Telephone Type" (see page 48) for more information on the tasks related to these privileges.			
Add Email/Telephone Types			X
Update Email/Telephone Types			X
List Email Types			
List Telephone Types			

Privilege	GA	OA	UA
Basic Authentication Privileges See "Specifying Basic Authentication Policy Settings" (see page 49) for more information on the tasks related to these privileges.			
Update Global Basic Authentication Policy		X	X
Update Organization Basic Authentication Policy			X
Encryption Privileges See "Configuring Attribute Encryption" (see page 41) for more information on the tasks related to these privileges.			
Configure the Encryption Set Selected			X
List Configured Attributes for Encryption			X
Case Management Privileges See "Managing Cases" (see page 309) for more information on the tasks related to these privileges.			
Manage Queues			X
Rebuild Queues			X
View Queue Status			X
Work on Cases			
Manage Inbound Calls			
Analyze Transactions			
RiskFort Configurations See "Managing Global Configurations" (see page 147) and "Managing Organization-Specific RiskMinder Configurations" (see page 259) for more information on the tasks related to these privileges.			
Create Ruleset			X
Assign Ruleset			X
Assign Channel and Configure Default Account Types		X	X
Manage Miscellaneous Configurations (global level)		X	X

Privilege	GA	OA	UA
Manage Miscellaneous Configurations (organization level)			X
Model Configuration (global level)		X	X
Model Configuration (organization level)		X	X
Configure RiskFort Callouts			X
Migrate to Production			X
Rule Management Privileges See "Managing Global Configurations" (see page 147) for more information on the tasks related to these privileges.			
Evaluate Risk			
List User Device Associations			
Delete User-Device Associations			
Manage List Data and Category Mappings			X
Rules and Scoring Management			X
Post Evaluate			
Other Privileges			
Get QnA Attributes			✓
Get QnA Values			
List Arcot Attributes			X
List Repository Attributes			X
Perform QnA Verification			
Bulk Upload			X
View Bulk Upload Requests			X

Privilege	GA	OA	UA
Report Privileges See "Generating Case Management Reports" (see page 342) and "Managing Reports" (see page 347) for more information on the tasks related to these privileges.			
View My Activity Report			
View User Activity Report			
View User Creation Report			
View Organization Report			X
View Administrator Activity Report			
Risk Detail Activity Report			
View Advice Summary Report			
View Exception User Report			
View Rules Configuration Report			X
View Rules Data Report and Category Mappings			X
Case Activity Report			X
Average Case Life Report			X
False Positives Report			
View Fraud Statistics Report			
Rule Effectiveness Report			
Reports Summary			

Chapter 4: Managing RiskMinder Server Instances

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

As a Master Administrator, you will need to manage a RiskMinder instance locally. However, before you can manage a server instance, you must configure the connectivity parameters to connect to the instance. For more information on this, see "Configuring Server Connectivity" (see page 66).

Only after you configure the connectivity parameters, you can manage the RiskMinder Server instance. The tasks for managing an instance include:

- Configuring Server Connectivity (see page 66)
- Creating Trust Stores (see page 71)
- Configuring Communication Protocols (see page 72)
- Configuring the RiskMinder Predictive Model (see page 77)
- Refreshing a Server Instance (see page 77)
- Updating Server Instance Configurations (see page 81)
- Shutting Down a Server Instance (see page 83)
- Restarting a Server Instance (see page 84)

Note: "Shutting Down a Server Instance" (see page 83) can also be performed by using system tools, as discussed in "Tools for System Administrators" **(see page 293).**

Configuring Server Connectivity

RiskMinder comprises two server components:

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

The following table lists the four sections on the RiskFort Connectivity page and describes the components that you can connect using each section.

Configuration Section	Description
RiskFort Server Management Connectivity	Used by Administration Console to connect to the RiskMinder Server Management port. For example, cache refresh and shutdown requests to RiskMinder Server.
Case Management Queuing Server Management Connectivity	Used by Administration Console to connect to the Case Management Queuing Server Management port. For example, cache refresh and shutdown requests to RiskMinder Server.
RiskFort Administration Connectivity	Used by Administration Console to connect to the RiskMinder Server Administration web service port. For example, the Rules and Scoring Management screen and Model Configuration screen.
Case Management Queuing Server Connectivity	Used by Administration Console to connect to the Case Management Queuing Server instance. For example, to issue Queue rebuild requests and to fetch the next case in the Queue.

RiskMinder Server Management Connectivity

You must use the RiskFort Server Management Connectivity section to configure the connection settings that will be used by Administration Console to connect to your RiskMinder Server Management instance.

To specify the connectivity parameters used by Administration Console to connect to the RiskMinder Server Management instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **RiskFort** link on the submenu of the tab.
4. If not already displayed, click the **RiskFort Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the RiskMinder connectivity parameters.

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

1. Click **Save** to save the configurations that you have set.

Case Management Queuing Server Management Connectivity

You must use the Case Management Queuing Server Management Connectivity section to configure the connection settings that will be used by Administration Console to connect to your Case Management Queuing Server Management instance.

To specify the connectivity parameters used by Administration Console to connect to the Case Management Queuing Server Management instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **RiskFort** link on the submenu of the tab.
4. If not already displayed, click the **RiskFort Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the RiskMinder connectivity parameters.

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

1. Click **Save** to save the configurations that you have set.

RiskMinder Administration Connectivity

You must use the RiskFort Administration Connectivity section to configure the connection settings that will be used by Administration Console to connect to your RiskMinder Server Administration instance.

To specify the connectivity parameters used by Administration Console to connect to the RiskMinder Server Administration instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **RiskFort** link on the submenu of the tab.
4. If not already displayed, click the **RiskFort Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the RiskMinder connectivity parameters.

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

1. Click **Save** to save the configurations that you have set.

Case Management Queuing Server Connectivity

You must use the Case Management Queuing Server Connectivity section to configure the connection settings that will be used by Administration Console to connect to your Case Management Queuing Server instance.

To specify the connectivity parameters used by Administration Console to connect to the Case Management Queuing Server instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **RiskFort** link on the submenu of the tab.
4. If not already displayed, click the **RiskFort Connectivity** link in the tasks pane to display the corresponding page.
5. Use the information in the following table to configure the RiskMinder connectivity parameters.

Field	Description
Host	Enter the IP address or host name of the system where you installed the Queuing Server instance. **Note:** Ensure that the system where Queuing Server is installed is accessible by its hostname on the network.
Backup Host	If installed, enter the IP address of the system where the backup Queuing Server instance is available. **Important!** You must configure this **Backup Host** parameter *before* you start the backup Case Management Queuing Server.
Port	Enter the port on which the Case Management service is exposed.
Transport	Specify the transport mode (**TCP** or **SSL**) for the corresponding component to connect to the specified Case Management instance: ■ Server Management Web Services ■ Administration Web Services ■ Transaction Web Services ■ Authentication Native
Server CA Root Certificate	Browse to and upload the server CA root certificate. **Note:** This server certificate must be in PEM format.

Field	Description
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store that contains the client certificate and the private key.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

1. Click **Save** to save the configurations that you have set.

Creating Trust Stores

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

You can use the Trusted Certificate Authorities page to create trust stores and to add new root certificates to your trust stores.

To create a trust store for your RiskMinder Server or Case Management Queuing Server instance:

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

Configuring Communication Protocols

The Protocol Configuration page allows you to configure protocols for the RiskMinder Server instance or the Case Management Queuing Server instance.

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

The following table explains the protocols that you see in the **List of Protocols** table for the RiskMinder Server instance and lists their default port numbers.

Protocol	Default Port Number	Description
Native (TCP)	7680	This is the protocol to enable communication between the RiskMinder Server instance and the RiskMinder Java SDKs, which include Risk Evaluation and Issuance (deprecated). **Note:** The Web service interface is available for Issuance as part of the user management Web Service Definition Language (WSDL).
Administration Web Service	7777	This is the protocol for communication between RiskMinder Server and Administration Web services. RiskMinder Server listens to the Administration Web service calls on this port. **Note:** These calls do *not* include the RiskMinder Issuance (deprecated) or Risk Evaluation calls.
Transaction Web Service	7778	This protocol is used by the Risk Evaluation and the Issuance (deprecated) Web services to connect to the RiskMinder Server instance. This protocol receives Web services requests that are sent by Authentication and Issuance Web services. **Note:** These calls do *not* include the Administration service calls.
Native (SSL)	7681	This is an binary protocol to enable SSL-based communication between the RiskMinder Server instance and the RiskMinder Java SDKs, which include Risk Evaluation and Issuance (deprecated).

Protocol	Default Port Number	Description
Server Management	7980	The arrfclient tool communicates with the RiskMinder Server instance for server management activities (graceful shutdown and server cache refresh) by using this protocol. See "arrfclient: Server Refresh and Shutdown Tool" (see page 299) for detailed information on this Administration Console tool.

Similarly, by selecting the Case Management Queuing Server instance from the drop-down list, you can configure the protocols that Administration Console and the Case Management Queuing Server use to communicate with your RiskMinder Server instance for authentication and administration purposes. In addition to the port on which the server listens to each of these enabled components, you can also specify the transport security mechanism (TCP or SSL). In case you specify this mechanism as SSL, then you must also specify the valid and trusted client component's certificate and private key that are required for establishing a secure connection.

The following table explains the protocols that you see in the **List of Protocols** table for the Case Management Queuing Server instance and lists their default port numbers.

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

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

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **RiskFort** tab in the submenu is displaye.
3. Under the **Instance Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page.
4. Select the RiskMinder Server instance or Case Management Queuing Server instance from the drop-down list.

   The **List of Protocols** appears.
5. In the **List of Protocols** table, click the link corresponding to the protocol that you want to configure.

   The corresponding Protocol page appears.
6. Edit the fields on the page, as required. The following table explains these fields.

Column	Action Description
Change Protocol Status	Select this check box to enable the **Action** drop-down list and change the status of the protocol.
Action	Select **Enable** to enable the required protocols. See the previous two tables for more information on the supported protocols.
Port	Enter the port number where the corresponding service is available. Following are the default port numbers for RiskMinder protocols: ■ **RiskFort Native (TCP):** 7680 ■ **RiskFort Native (SSL):** 7681 ■ **Administration Web Services:** 7777 ■ **Transaction Web Services:** 7778 ■ **Queuing Server:** 7779 ■ **Queuing Administration:** 7780 ■ **Server Management:** 7980
Minimum Threads	Minimum number of threads processed on the port.
Maximum Threads	Maximum number of threads processed on the port.

Column	Action Description
Transport	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 RiskMinder protocols. It sends data in the clear. ■ **SSL:** Secure Sockets Layer (SSL) provides higher security for transactions, because it encrypts and decrypts data that is transmitted.
Key in HSM	Enable this check box if the private key for the SSL communication needs to be in the HSM device. In this case, RiskMinder Server and Case Management Queuing Server will find the private key based on the certificate chain provided. This checkbox is enabled only if you select **SSL** in "Transport".
Server Certificate Chain	Specify the certificate chain that is used by the SSL transport security mode. Use the **Browse** button to upload the **Server Certificate Chain**. **Important!** Ensure that the certificates in the chain that you upload here follow the Leaf certificate --> Intermediate CA certificates --> Root certificate hierarchy. The certificate and the key must be in PEM format.
Server Private Key	Use the **Browse** button to upload the **Server Private Key**. **Note:** This field will be enabled only if you did not select the **Key in HSM** check box.
Select Client Store	Select the trust store that contains the root certificates of the trusted CAs. See "Creating Trust Stores" (see page 71) for more information on configuring trust stores.

1. Click **Save** after you complete the configurations on the page.

(Optional) Configuring SSL Communication

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

Note: See "Configuring SSL" (see page 85) for step-by-step configuration of SSL-based communication between different RiskMinder components.

If you have configured SSL for secure communication, you can see the corresponding entries in the startup log files. The following table lists the log file entries when SSL is configured for RiskMinder Server and Case Management Queuing Server protocols.

Protocol	**Entry in Log File**
RiskMinder	
Server Management	Started listener for [Server Management] [7980] [SSL] [srvmgrwsprotocol]
Transaction Web Service	Started listener for [RiskFort Trans WS] [7778] [SSL] [transwsprotocol]
Administration Web Service	Started listener for [RiskFort Admin WS] [7777] [SSL] [aradminwsprotocol]
Native (SSL)	Started listener for [RiskFort Native (SSL)] [7681] [SSL] [RiskFort]
Case Management Queuing Server	
Case Management Queuing Administration	Started listener for [Case Management Admin] [7780] [SSL] [srvmgrwsprotocol]
Case Management Queuing Server	Started listener for [Case Management Server] [7779] [SSL] [RiskFortCaseManagement]

Configuring the RiskMinder Predictive Model

You can configure the URL and timeout parameters for the RiskMinder Predictive Model using Administration Console.

To configure the RiskMinder Predictive Model:

1. Ensure that you are logged in as a MA.
2. Activate the **Services and Server Configurations** tab.
3. Activate the **RiskFort** tab.
4. Under the **Model Configuration** section on the side-bar menu, click the **Model Configuration** link.

   The Model Configuration page appears.
5. In the **Proposed Value** column, specify the parameters as described in the following table.

Parameter	Description
Predictive Model URL (primary)	The primary URL of the RiskMinder Predictive Model.
Predictive Model URL (backup)	The backup URL of the RiskMinder Predictive Model.
Connection Timeout (in milliseconds)	The time in which connection between RiskMinder Server and the Predictive Model will expire.
Read Timeout (in milliseconds)	The time in which RiskMinder Server expects a response back from the Predictive Model.
Minimum Connections	The minimum number of connections in the connection pool to connect to the Model Server.
Maximum Connections	The maximum number of connections in the connection pool to connect to the Model Server.

6. Click **Upload Model Configuration** to save the changes.
7. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Refreshing a Server Instance

You can refresh RiskMinder Server and the Case Management Queuing Server instances either through Administration Console or by using the arrfclient tool.

Using Administration Console to Refresh Server Instances

You can refresh specific RiskMinder Server and the Case Management Queuing Server instances by selecting the instance on the Instance Management page.

To refresh server instances:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **RiskFort** tab in the submenu is displayed.
3. Under the **Instance Configuration** section, click the **Instance Management** link to display the page.

   The following table describes the columns on the Instance Management page.

Column	Description
Instance Name	Name of RiskMinder Server or the Case Management Queuing Server instance.
Last Startup Time	The time the instance was last started.
Last Shut Down Time	The time the instance was last shut down.
Last Refresh Time	The time the instance was last refreshed.
Uptime	The duration for which the instance has been running.
Status	The status of the instance.
Organization List To Refresh	The list of organizations to refresh. ■ Choose **Select** in the drop-down list to select the organizations that you want to refresh. or ■ Select **All** in the drop-down list to refresh all organizations.
System Cache Refresh	Select this check box to refresh the system cache.

1. In the **RiskFort Instances** section:
   a. Select the instance of RiskMinder Server that you want to refresh.
   b. Select the organizations to refresh from the **Organization List to Refresh** drop-down list.
   c. Select **System Cache Refresh** if you want to refresh the system cache configuration.
   d. Click **Refresh**.
2. In the **Case Management Instances** section:
   a. Select the instance of the Case Management Queuing Server that you want to refresh.
   b. Select the organizations to refresh from the **Organization List to Refresh** drop-down list.
   c. Select **System Cache Refresh** if you want to refresh the system cache configuration.
   d. Click **Refresh**.

Using the arrfclient Tool to Refresh Server Instances

You can use the arrfclient tool to refresh both RiskMinder Server and the Case Management Queuing Server instances.

Important! Before you run the arrfclient tool for RiskMinder Server as directed in the following subsections, set the Host and Port values in riskfortadminclient.ini. See "arrfserver: RiskMinder Server Tool" (see page 302) for more information.

See "arrfclient: Server Refresh and Shutdown Tool" (see page 299) for more information on the tool.

On Windows

Run the arrfclient tool to refresh the RiskMinder Server cache as follows:

1. Open the Command Prompt window.
2. Navigate to the following directory:
   `<install_location>\Arcot Systems\bin\`
3. Run the following command to refresh:
   - **RiskMinder Server instance:**
     `arrfclient -cr`
   - **Case Management Queuing Server instance:**
     `arrfclient <host_name> CA Portal -cr`

On UNIX-Based Platforms

Run the arrfclient tool to refresh the RiskMinder Server cache as follows:

1. Open the terminal window.
2. Navigate to the following directory:
   `<install_location>/arcot/bin/`
3. Run the following command to refresh:
   - **RiskMinder Server instance:**
     `arrfclient -cr`
   - **Case Management Queuing Server instance:**
     `arrfclient <host_name> CA Portal -cr`

Updating Server Instance Configurations

You can update the instance attributes, logging configurations, and database configurations for the RiskMinder Server and Case Management Queuing Server instances.

To update instance-specific configurations:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **RiskFort** tab in the submenu is active.
3. Under the **Instance Configuration** section, click the **Instance Management** link to display the page.
4. Click the link corresponding to the instance whose configuration you want to update.

   The page to update the instance-specific configuration appears.
5. In the **Instance Attributes** section:
   a. Select the check box to **Change the Instance Name** of your RiskMinder Server or Case Management Queuing Server instance.
   b. Specify name for the instance in the **New Instance Name** field.
6. In the **Logging Configuration** section, specify values as described in the following table.

Field	Description
Transaction Log Directory	The directory to store the transaction log files. The path can be an absolute path or relative to ARCOT_HOME.
Rollover After (in Bytes)	The maximum number of bytes the log file can contain. When the log files reach this size, a new file with the specified name is created and the old file is moved to the backup directory.
Transaction Log Backup Directory	The backup directory to store the older transaction log files. The path can be an absolute path or relative to ARCOT_HOME.
Log Level	The severity level of the logged entry. Fatal, WARNING, INFO, and DETAIL are the supported levels in decreasing order of severity. See "Supported Severity Levels" (see page 399) in appendix for more information.

Field	Description
Log Timestamps in GMT	Select this option if you want to time stamp the logged information using GMT. RiskMinder enables you to either use the local time zone or GMT to timestamp the logged information.
Enable Trace Logging	An additional logging flag that logs the Entering and Exiting log for each function called during processing. By default, this flag is disabled. Enabling this flag logs huge amount of data for debugging. You must not enable this flag in production unless advised by CA Support.

7. In the **Database Configurations** section, specify values as described in the following table.

Field	Description
Minimum Connections	The minimum number of connections that will be created between RiskMinder Server and the database.
Maximum Connections	The maximum number of connections that can be created between RiskMinder Server and the database.
Increment Connections by	The value by which to increment the connections when all database connections in the pool are exhausted and used by the existing threads, and if any of the threads requests for a new database connection.
Monitor Thread Sleep Time (in Seconds)	The time interval after which the database monitor thread polls the database to check if the database is active and functional.
Monitor Thread Sleep Time in Fault Conditions (in Seconds)	Same as Monitor Thread Sleep Time. But this value is used only when the database monitor thread detects any failure. This value *must* be less than the Monitor Thread Sleep Time because polling must be done at frequent intervals in the case of any failure.
Log Query Details	When enabled, this option logs all the Oracle, MS SQL, or MySQL database queries executed by the Server. By default, this option is disabled and must be enabled *only* when debugging is required as in the case of Enable Trace Logging.
Monitor Database Connectivity	If this option is enabled, the Server creates the database monitor thread. Else, database monitoring is disabled.

Field	Description
Auto-Revert to Primary	When the connection to the primary database fails, the Server falls back to the backup database. If this option is enabled, the Server automatically reverts to the primary database when it is up and running.

8. Click **Save** to save your changes.
9. Refresh or restart your server instance depending on the parameters that you have updated.

   For instructions on how to do this, see "Refreshing a Server Instance" (see page 77) and "Restarting a Server Instance" (see page 84).

Shutting Down a Server Instance

To shut down a RiskMinder Server or Case Management Queuing Server instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu, and ensure that the **RiskFort** tab in the submenu is displayed.
3. Under the **Instance Configuration** section, click the **Instance Management** link to display the page.
4. Select a RiskMinder Server instance or a Case Management Queuing Server instance that you want to shut down.
5. Click **Shut Down** to shut down the selected server instances.

Note: When a shutdown request is received by RiskMinder Server, all the ongoing transactions are processed, and then the shutdown request is processed.

Restarting a Server Instance

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

On Windows

To start a server instance on Windows:

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

On UNIX-Based Platforms

To start a server instance on UNIX-based platforms:

1. Log in to the computer where the instance must be started.
2. Navigate to the following directory:
   `<install_location>/arcot/bin/`
3. Run the following command to restart:
   - **RiskMinder Server instance:**
     `./riskfortserver start`
   - **Case Management Queuing Server instance:**
     `./casemanagementserver start`

Chapter 5: Configuring SSL

By default, RiskMinder components use Transmission Control Protocol (TCP) to communicate with each other. To ensure secure communication between Administration Console and RiskMinder Server and between SDKs and RiskMinder Server, you can configure RiskMinder Native and Server Management protocols to support SSL (Secure Socket Layer), which ensures secure communication between applications across insecure media.

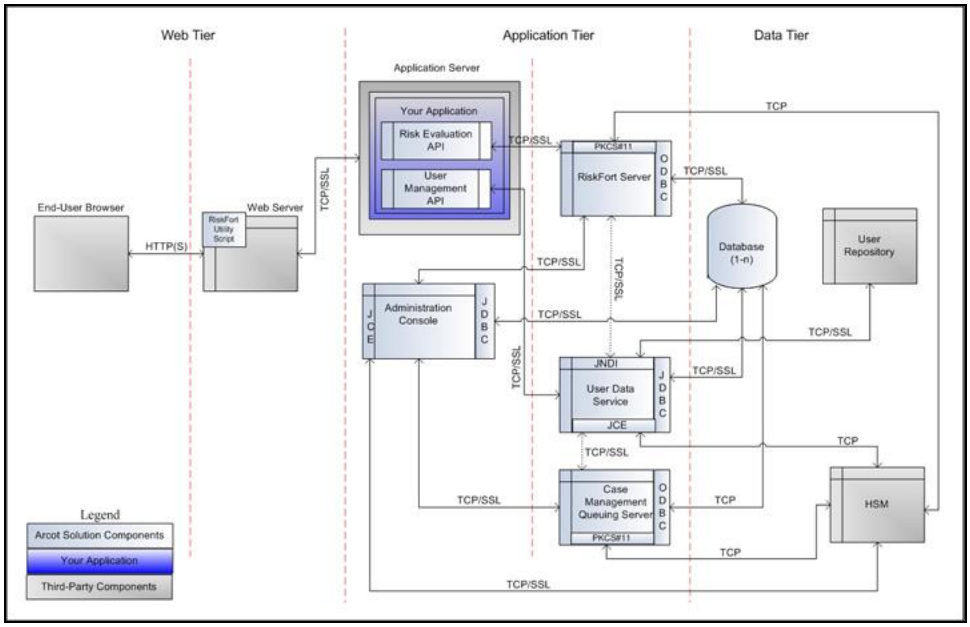
The steps to set up SSL between different components of RiskMinder include:

Note: You *must* follow this order to set up SSL successfully. After completing every step, test whether connection has been set successfully.

1. Prepare for SSL Communication (see page 87)
2. Enable SSL Between RiskMinder Server and User Data Service (see page 93)
3. Enable SSL Between Case Management Queuing Server and User Data Service (see page 96)
4. Enable SSL Between Administration Console and RiskMinder Server (see page 97)
5. Enable SSL Between Administration Console and Case Management Queuing Server (see page 108)
6. Enable SSL Between Java SDK and RiskMinder Server (see page 118)
7. Enable SSL Communication Between Risk Evaluation Web Service and RiskMinder Server (see page 123)
8. Enable SSL Communication Between Administration Web Service and RiskMinder Server (see page 126)
9. Enable One-Way SSL Between RiskMinder Components and Database (see page 129)

RiskFort Components and Their Communication Modes

The following figure illustrates the possible communication modes that are supported between RiskMinder and its components.



As shown in this figure, the default mode of communication between components is TCP, RiskMinder Server supports SSL communication (two-way as well as one-way) with the following components to ensure integrity and confidentiality of the data being exchanged during a transaction:

- Case Management Queuing Server
- RiskMinder Database
- User Data Service
- RiskMinder SDKs (Risk Evaluation)
- Sample Application
- Evaluation Callout
- Scoring Callout

RiskMinder supports one-way SSL as well as two-way SSL communication between components.

Prepare for SSL Communication

To enable SSL communication between the RiskMinder components, you must first obtain server and client certificates. You can obtain these certificate by using one of the following methods:

- Obtaining Certificates Directly Through a Certificate Authority (CA) (see page 88)
- Generating Certificate Requests by Using a Utility (see page 92)

When a CA generates a certificate for you (as discussed in section, "Obtaining Certificates Directly Through a Certificate Authority (CA)" (see page 88)), they also generate the private key associated with the certificate. As a result, the private key might not be as secure as when it is generated at your end. If you do not want the key to be generated "off site", then you must follow the steps in "Generating Certificate Requests by Using a Utility" (see page 92).

Obtaining Certificates Directly Through a Certificate Authority (CA)

Note: The steps that are explained in this section are specific to **Microsoft CA 2008**. If you are using any other CA to generate the certificate and the private key, then you must refer to the vendor documentation.

To generate a CA-issued certificate:

1. Access the link to the CA of your choice. For Microsoft CA, it is as follows:

   http://<IP_Address_of_the_CA>/certsrv/

2. Navigate to the link to create and submit the certificate request.

   For example, if you are using **MSCA**, then under **Select a task** section, click the **Request a certificate** option, then **advanced certificate request** option, and then finally the **Create and submit a request to this CA** option.

3. Specify the details on the certificate request form that appears.

   - The identification information for the certificate, as described in the following table.

Certificate Attribute	Required Information
Common Name (Name)	The fully qualified domain name (FQDN) of your server. **Important!** When prompted for Common Name, you *must* specify the Fully Qualified Domain Name (FQDN) of the server to be protected by SSL. For example, an SSL certificate issued for login.my-bank.com will *not* be valid for online.my-partner.com. If the URL to be used for SSL is login.my-bank.com, then ensure that the common name submitted in the CSR is login.my-bank.com.
Email Address	The email ID of the contact person in your organization. **Note:** Typically, this is the email address of the certificate administrator or an administrator in the IT department.
Organization (Company)	The name of your organization. **Important!** Ensure that this entry is *not* abbreviated. You must also ensure that you do not specify any suffixes, such as Inc., Corp., or LLC.

Certificate Attribute	Required Information
Organizational Unit (Department)	The division (for example, IT) of your Organization handling the certificate.
City (Locality)	The city (for example, Brisbane) where your Organizational Unit is located.
State	The state or region (for example, Queensland) where your Organizational Unit is located. **Important!** Ensure that this entry is not abbreviated.
Country (Region)	The ISO code (for example, AU) for the country where your organization is headquartered.

- The details of the certificate. You must consider the details specified in the following table while specifying these certificate details.

Certificate Attribute	Required Information
Certificate Type	**Server Authentication Certificate**, if you are generating a server certificate **Client Authentication Certificate**, if you are generating a client certificate
CSP	CSP of your choice
Key Usage	Exchange
Key Size	The key size in bytes.
Key Exportability	■ Mark keys as exportable ■ Export keys to file ■ Full path name (*.pvk)
Request Format	PKCS#12 File

1. Click **Submit** to request the certificate.
2. Click **Install the Certificate** to install the certificate in the browser store.

Download Certificates

The certificates that you requested through Microsoft CA 2008 are installed in the browser store, from where you have to download them. The format in which you have to download the certificate depends on the encryption mode:

- If software encryption is used, then certificates must be In PKCS#12 Format.
- If hardware encryption is used, then certificates must be In PEM Format.

In PKCS#12 Format

To download the certificate and private key to a PKCS#12 file by using Microsoft CA 2008:

1. Open an Internet Explorer window.
2. Navigate to **Tools** and then **Internet Options**.

   The Internet Options dialog box appears.
3. Activate the **Content** tab, in the Certificates section click **Certificates**.

   The Certificates dialog box appears.
4. Select the certificate that you want to download and click **Export**.

   The Certificate Export Wizard appears.
5. Click **Next** on the Welcome screen.
6. Choose **Yes, export the private key** option, and click **Next**.
7. Ensure that the **Personal Information Exchange - PKCS # 12 (.PFX)** option is selected.
8. Select **Enable Strong Protection** option, and click **Next**.
9. Enter the password for the PKCS#12 (.PFX) file in the **Password** and **Confirm password** fields, and click **Next**.
10. Enter the **File name** with which you want to download the PKCS#12 (.PFX) file and click **Next**.
11. Click **Finish** to complete the wizard.

    The certificate and private key are now available on your system in the specified location.

In PEM Format

You cannot directly export the certificate in .PEM format from the browser certificate store. As a result, you must first download it in .DER format (by using Microsoft CA 2008) and then convert to .PEM as follows:

1. Open an Internet Explorer window.
2. Navigate to **Tools** and then **Internet Options**.

The Internet Options dialog box appears.

3. Activate the **Content** tab, in the Certificates section click **Certificates**.

   The Certificates dialog box appears.

4. Select the certificate that you want to download and click **Export**.

   The Certificate Export Wizard appears.

5. Click **Next** on the Welcome screen.
6. Choose **No, do not export the private key** option and then **Next**.
7. Ensure that the **DER encoded binary X.509 (.CER)** option is selected.
8. Click **Next**.
9. Enter the **File name** with which you want to download the certificate, and click **Next**.
10. Click **Finish** to complete the wizard.

    The certificate is now available on your system in the specified location.

11. Convert DER to PEM format.

    To convert the certificate from DER to PEM format, you can use open source tools such as OpenSSL. Use the following command to convert using OpenSSL tool:
    `openssl x509 -inform der -in <certificate>.cer -out <certificate>.pem`

Generating Certificate Requests by Using a Utility

You can also generate a certificate by using any utility or tool of your choice. The keytool utility (which is available with JDK) has been used for the following operations:

1. Generate the keystore.

   keytool stores the keys and certificates in a file termed a *keystore*, which is a repository of certificates used for identifying a client or a server. Typically, a keystore is specific to one client or one server. The default keystore implementation implements the keystore as a file. It protects private keys by using a password. The keystores are created in the directory from which you run keytool.

   Use the following command to generate the keystore:
   `$%JAVA_HOME%/\bin/\keytool -genkey -keyalg RSA -alias <server/or/client> -keystore <keystore_name>.jks -storetype JKS -storepass <password> -keysize 1024 -validity <validity_period_in_days>`

2. Generate the Certificate Signing Request (CSR).

   CSR is encrypted identification text (see the first table in Obtaining Certificates Directly Through a Certificate Authority (CA) (see page 88)), and must be generated on the system where the certificate will be used. A private key is usually created at the same time that you create the CSR.

   Use the following command to generate the CSR:
   `$%JAVA_HOME%/\bin/\keytool -certreq -v -alias <server/or/client> -keystore <keystore_name>.jks -storepass <password> -file <server/or/client>certreq.csr`

3. Generate the certificate by submitting the CSR generated in the preceding step to a CA.

   a. Access the link to the CA of your choice.

      For example, if you are using **MSCA**, then the link will be similar to:

      http://<IP_Address_of_the_CA>/certsrv/

   b. Navigate to the link to create and submit the certificate request.

      For example, if you are using **MSCA**, then under **Select a task** section, click the **Request a certificate** option, then **advanced certificate request** option, and then the **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file** option (or if you are renewing the certificate, then submit a renewal request by using a base-64-encoded PKCS #7 file). Finally, copy and paste the contents of <*server/or/client*>clientcertreq.csr in the **Base-64-encoded certificate request** field and click **Submit**.

   c. Download the following files in the Base-64-encoded format:

      - Signed certificate as clientcert.cer
      - Complete certficate chain as clientcertchain.p7b
      - CA certficate as clientcacert.cer

4. Import the certificate chain in to keystore.

   Use the following command to do so:
   ```
   $%JAVA_HOME%/\bin/\keytool -import -keystore
   <server/or/client>keystore.jks -storepass <password> -file
   <server/or/client>certchain.p7b -alias <server/or/client>
   ```

5. Convert the certificates or keystore to the required formats:

   - From DER Format

     - To convert DER format to PEM, use the following command:

     ```
     openssl x509 -inform der -in <server/or/client>cert.cer -out
     <server/or/client>cert.pem
     ```

     - To convert DER format to PKCS#12, first convert DER to PEM using the preceding command, and then convert PEM to PKCS#12 use the following command:

     ```
     openssl pkcs12 -export -out <server/or/client>cert.pfx -inkey
     privateKey.key -in <server/or/client>cert.cer -certfile
     <server/or/client>cacert.cer
     ```

   - From P7B Format

     - To convert P7B format to PEM, use the following command:

     ```
     openssl pkcs7 -print_certs -in <server/or/client>cert.p7b -out
     <server/or/client>cert.cer
     ```

     - To convert P7B format to PKCS#12, first convert P7B to PEM using the preceding command, and then convert PEM to PKCS#12 use the following command:

     ```
     openssl pkcs12 -export -in <server/or/client>cert.cer -inkey
     privateKey.key -out <server/or/client>cert.pfx -certfile
     <server/or/client>cacert.cer
     ```

Enable SSL Between RiskMinder Server and User Data Service

To set up SSL between RiskMinder Server and User Data Service (UDS), you must upload the UDS Server certificates required for SSL communication by using the **User Data Service Connectivity Configuration** page of Administration Console. In case of two-way SSL, you must also upload the RiskMinder Server client certificate by using the **User Data Service Connectivity Configuration** page. The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 94)
- Two-Way SSL (see page 95)

One-Way SSL

To enable one-way SSL communication between RiskMinder Server and UDS:

1. Enable the application server where User Data Service (UDS) is deployed for SSL communication.

   Refer to your application server vendor documentation for more information on how to do this.

2. Access Administration Console in a Web browser window.
3. Log in to Administration Console as the Master Administrator (MA).
4. Activate the **Services and Server Configurations** tab.
5. Activate the **Administration Console** subtab to display the User Data Service Connectivity Configuration page.
6. From the **Protocol** list, select **One-Way SSL**.
7. Set the **Port** value to default SSL port.
8. Click the **Browse** button adjacent to the **Server Root Certificate** field to navigate to and select the UDS root certificate.
9. Click **Save**.
10. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

Two-Way SSL

To set up two-way SSL between RiskMinder Server and User Data Service (UDS):

1. Enable the application server where User Data Service (UDS) is deployed for SSL communication.

   Refer to your application server vendor documentation for more information on how to do this.

2. Access Administration Console in a Web browser window.
3. Log in to Administration Console as the MA.
4. Activate the **Services and Server Configurations** tab.
5. Activate the **Administration Console** subtab to display the User Data Service Connectivity Configuration page.
6. From the **Protocol** list, select **Two-Way SSL**.
7. Set the **Port** value to the default SSL port.
8. Click the **Browse** button adjacent to the **Server Root Certificate** field to navigate to and select the UDS root certificate.
9. Click the **Browse** button adjacent to the **Client Certificate** field to navigate to select the RiskMinder root certificate.
10. Click the **Browse** button adjacent to the **Client Private Key** field to select the RiskMinder Server private key.
11. Click **Save**.
12. Restart RiskMinder Server:

    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

Enable SSL Between Case Management Queuing Server and User Data Service

To set up SSL between Case Management Queuing Server and User Data Service (UDS), you must upload the UDS Server certificates required for SSL communication by using the **User Data Service Connectivity Configuration** page of Administration Console. In case of two-way SSL, you must also upload the Case Management Queuing Server client certificate by using the **User Data Service Connectivity Configuration** page. The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 96)
- Two-Way SSL (see page 97)

One-Way SSL

To enable one-way SSL communication between Case Management Queuing Server and UDS:

1. Enable the application server where User Data Service (UDS) is deployed for SSL communication.

   Refer to your application server vendor documentation for more information on how to do this.
2. Access Administration Console in a Web browser window.
3. Log in to Administration Console as the Master Administrator (MA).
4. Activate the **Services and Server Configurations** tab.
5. Activate the **Administration Console** subtab to display the User Data Service Connectivity Configuration page.
6. From the **Protocol** list, select **One-Way SSL**.
7. Set the **Port** value to default SSL port.
8. Click the **Browse** button adjacent to the **Server Root Certificate** field to navigate to and select the UDS root certificate.
9. Click **Save**.
10. Restart the Case Management Queuing Server instance:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.

Two-Way SSL

To set up two-way SSL between Case Management Queuing Server and User Data Service (UDS):

1. Enable the application server where User Data Service (UDS) is deployed for SSL communication.

   Refer to your application server vendor documentation for more information on how to do this.

2. Access Administration Console in a Web browser window.
3. Log in to Administration Console as the MA.
4. Activate the **Services and Server Configurations** tab.
5. Activate the **Administration Console** subtab to display the User Data Service Connectivity Configuration page.
6. From the **Protocol** list, select **Two-Way SSL**.
7. Set the **Port** value to default SSL port.
8. Click the **Browse** button adjacent to the **Server Root Certificate** field to navigate to and select the UDS root certificate.
9. Click the **Browse** button adjacent to the **Client Certificate** field to navigate to select the Case Management Queuing Server root certificate.
10. Click the **Browse** button adjacent to the **Client Private Key** field to select the Case Management Queuing Server private key.
11. Click **Save**.
12. Restart the Case Management Queuing Server instance:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.

Enable SSL Between Administration Console and RiskMinder Server

This section walks you through the steps for SSL configuration between Administration console and RiskMinder Server:

- For Server Refresh, Restart, Instance Management, and Protocol Management Activities (see page 98)
- For Rule Configurations Activities (see page 103)

For Server Refresh, Restart, Instance Management, and Protocol Management Activities

RiskMinder Server listens to server management activities such as, graceful shutdown, server cache refresh, instance management from Administration Console by using the Server Management port (7980).

To set up SSL between Administration Console and RiskMinder Server for the server management activities, you must configure the Server Management port (7980) for SSL and provide the corresponding Server Root CA Certificate on the RiskFort Connectivity page. Additionally, if two-way SSL is required, you must upload the **Client Certificate-Key Pair in PKCS#12** file on the RiskFort Connectivity page and select the appropriate trust store on the Protocol Configuration page for this port.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 99)
- Two-Way SSL (see page 101)

One-Way SSL

To set up one-way SSL communication between Administration Console and RiskMinder Server for server management activities:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** subtab is activated.
5. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
6. Select the **Server Instance** for which you want to configure SSL communication.
7. In the **List of Protocols** section, click the **Server Management** link.

   The page to configure the Server Management protocol appears.
8. Configure the following fields:
   - Ensure that the **Protocol Status** is **Enabled**.

     If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
   - Ensure that the **Port** is set to the correct SSL port value.
   - Select **SSL** from the **Transport** list.
   - If you want to store the SSL key on HSM, then select the **Key in HSM** option.
   - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
   - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
9. Click the **Save** button.
10. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
11. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
12. In the **RiskFort Server Management Connectivity** section:
    - Ensure that the IP address or the host name of RiskMinder Server is correctly set in the **Server** field.

- Ensure that the **Server Management Port** is also set to point the RiskMinder Server port that is open to Server Management requests.
- Select **SSL** from the **Transport** list.
- Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the RiskMinder root certificate.

13. Click the **Save** button.
14. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
15. Restart Administration Console.

Two-Way SSL

To set up two-way SSL communication between Administration Console and RiskMinder Server for server management activities:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** tab is active.
5. Under **System Configuration**, click the **Trusted Certificate Authorities** link to display the Riskfort Server Trusted Certificate Authorities page.
6. Set the following information on the page:
   - In the **Name** field, enter the name for the SSL truststore.
   - Click the **Browse** button adjacent to the first **Root CAs** field and navigate to and select the root certificate of the application server where Administration Console is deployed.
7. Click the **Save** button.
8. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
9. Select the **Server Instance** for which you want to configure SSL communication.
10. In the **List of Protocols** section, click the **Server Management** link.

    The page to configure the Server Management protocol appears.
11. Configure the following fields:
    - Ensure that the **Protocol Status** is **Enabled**.

      If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
    - Ensure that the **Port** is set to the correct SSL port value.
    - Select **SSL** from the **Transport** list.
    - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
    - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
    - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
    - **Select Client Store** that you created in Step 6.
12. Click the **Save** button.
13. Restart RiskMinder Server:

- **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
- **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

14. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
15. On the RiskFort Connectivity page:
    - Ensure that the IP address or the host name of RiskMinder Server is correctly set in the **Server** field.
    - Ensure that the **Server Management Port** is also set to point the RiskMinder Server port that is open to Server Management requests.
    - Select **SSL** from the **Transport** list.
    - Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the RiskMinder root certificate.
    - Click the **Browse** button adjacent to the **Client Certificate-Key Pair in PKCS#12** field to navigate to and select the root certificate of the application server where Administration Console is deployed.
    - Enter the PKCS#12 file password in the **Client PKCS#12 Password** field.
16. Click the **Save** button.
17. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
18. Restart Administration Console.
19. Verify that RiskMinder Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
    b. Open the arcotriskfortstartup.log file in a text editor.
    c. Check for the following line:
    ```
    Started listener for [Server Management] [7980] [SSL]
    [srvmgrwsprotocol]
    ```
    If you located this line, then two-way SSL was set successfully.
    d. Close the file.

For Rule Configurations Activities

RiskMinder Server listens to rules configuration requests (such as, adding a user to Exception User List or deleting a user from Exception User List and viewing user profile or connection information) from Administration Console by using the Administration Web Service port (7777).

To set up SSL between Administration Console and RiskMinder Server for the rule configuration activities, you must configure the Administration Web Service port (7777) for SSL and provide the corresponding Server Root CA Certificate on the RiskFort Connectivity page. Additionally, if two-way SSL is required, you must upload the **Client Certificate-Key Pair in PKCS#12** file on the RiskFort Connectivity page and select the appropriate trust store on the Protocol Configuration page for this port.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 99)
- Two-Way SSL (see page 101)

One-Way SSL

To set up one-way SSL communication between Administration Console and RiskMinder Server for administrative activities:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** subtab is activated.
5. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
6. Select the **Server Instance** for which you want to configure SSL communication.
7. In the **List of Protocols** section, click the **Administration Web Service** link.

   The page to configure the Administration Web Service protocol appears.
8. Configure the following fields:
   - Ensure that the **Protocol Status** is **Enabled**.

     If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
   - Ensure that the **Port** is set to the correct SSL port value.
   - Select **SSL** from the **Transport** list.
   - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
   - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
   - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
9. Click the **Save** button.
10. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
11. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
12. Scroll down to the **RiskFort Administration Connectivity** section.
13. In the **RiskFort Administration Connectivity** section:

- Ensure that the IP address or the host name of RiskMinder Server is correctly set in the **Server** field.
- Ensure that the **Server Management Port** is also set to point the RiskMinder Server port that is open to Administration Web Service requests.
- Select **SSL** from the **Transport** list.
- Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the RiskMinder root certificate.

14. Click the **Save** button.
15. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
16. Restart Administration Console

Two-Way SSL

To set up two-way SSL communication between Administration Console and RiskMinder Server for administrative activities:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** tab is active.
5. Under **System Configuration**, click the **Trusted Certificate Authorities** link to display the Riskfort Server Trusted Certificate Authorities page.
6. Set the following information on the page:
   - In the **Name** field, enter the name for the SSL truststore.
   - Click the **Browse** button adjacent to the first **Root CAs** field and navigate to and select the root certificate of the application server where Administration Console is deployed.
7. Click the **Save** button.
8. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
9. Select the **Server Instance** for which you want to configure SSL communication.
10. In the **List of Protocols** section, click the **Administration Web Service** link.

    The page to configure the Administration Web Service protocol appears.
11. Configure the following fields:
    - Ensure that the **Protocol Status** is **Enabled**.

      If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
    - Ensure that the **Port** is set to the correct SSL port value.
    - Select **SSL** from the **Transport** list.
    - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
    - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
    - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
    - **Select Client Store** that you created in Step 6.
12. Click the **Save** button.
13. Restart RiskMinder Server:

- **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
- **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

14. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
15. On the RiskFort Connectivity page, under the **RiskFort Administration Connectivity** section:
    - Ensure that the IP address or the host name of RiskMinder Server is correctly set in the **Server** field.
    - Ensure that the **Server Management Port** is also set to point the RiskMinder Server port that is open to Server Management requests.
    - Select **SSL** from the **Transport** list.
    - Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the RiskMinder root certificate.
    - Click the **Browse** button adjacent to the **Client Certificate-Key Pair in PKCS#12** field to navigate to and select the root certificate of the application server where Administration Console is deployed.
    - Enter the PKCS#12 file password in the **Client PKCS#12 Password** field.
16. Click the **Save** button.
17. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
18. Restart Administration Console.
19. Verify that RiskMinder Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
    b. Open the arcotriskfortstartup.log file in a text editor.
    c. Check for the following line:
    ```
    Started listener for [RiskFort Admin WS] [7777] [SSL]
    [aradminwsprotocol]
    ```
    If you located this line, then two-way SSL was set successfully.
    d. Close the file.

Enable SSL Between Administration Console and Case Management Queuing Server

This section walks you through the steps for SSL configuration between Administration Console and Case Management Queuing Server:

- For Server Refresh and Restart Activities (see page 108)
- For Fetching Cases (see page 113)

For Server Refresh and Restart Activities

Case Management Queuing Server listens to server management activities such as, graceful shutdown and server cache refresh from Administration Console by using the Case Management Queuing Administration port (7780).

To set up SSL between Administration Console and Case Management Queuing Server for the server management activities, you must configure the Server Management port (7780) for SSL and provide the corresponding Server Root CA Certificate on the RiskFort Connectivity page. Additionally, if two-way SSL is required, you must upload the **Client Certificate-Key Pair in PKCS#12** file on the RiskFort Connectivity page and select the appropriate trust store on the Protocol Configuration page for this port.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 109)
- Two-Way SSL (see page 111)

One-Way SSL

To set up one-way SSL communication between Administration Console and Case Management Queuing Server for server management activities:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** subtab is activated.
5. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
6. Select the **Server Instance** for which you want to configure SSL communication.
7. In the **List of Protocols** section, click the **Case Management Queuing Administration** link.

   The page to configure the Case Management Queuing Administration protocol appears.
8. Configure the following fields:
   - Ensure that the **Protocol Status** is **Enabled**.

     If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
   - Ensure that the **Port** is set to the correct SSL port value.
   - Select **SSL** from the **Transport** list.
   - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
   - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the Case Management Queuing Server root certificate.
   - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the Case Management Queuing Server private key.
9. Click the **Save** button.
10. Restart Case Management Queuing Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.
11. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
12. In the **Case Management Queuing Server Management Connectivity** section:

- Ensure that the IP address or the host name of Case Management Server is correctly set in the **Server** field.
- Ensure that the **Server Management Port** is also set to point the Case Management Server port that is open to server management requests.
- Select **SSL** from the **Transport** list.
- Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the Case Management Server root certificate.

13. Click the **Save** button.
14. Restart Case Management Queuing Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.
15. Restart Administration Console.

Two-Way SSL

To set up two-way SSL communication between Administration Console and Case Management Queuing Server for server management activities:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** tab is active.
5. Under **System Configuration**, click the **Trusted Certificate Authorities** link to display the Riskfort Server Trusted Certificate Authorities page.
6. Set the following information on the page:
   - In the **Name** field, enter the name for the SSL truststore.
   - Click the **Browse** button adjacent to the first **Root CAs** field and navigate to and select the root certificate of the application server where Administration Console is deployed.
7. Click the **Save** button.
8. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
9. Select the **Server Instance** for which you want to configure SSL communication.
10. In the **List of Protocols** section, click the **Case Management Queuing Administration** link.

    The page to configure the Case Management Queuing Administration protocol appears.
11. Configure the following fields:
    - Ensure that the **Protocol Status** is **Enabled**.

      If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
    - Ensure that the **Port** is set to the correct SSL port value.
    - Select **SSL** from the **Transport** list.
    - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
    - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the Case Management Server root certificate.
    - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the Case Management Server private key.
    - **Select Client Store** that you created in Step 6.
12. Click the **Save** button.

13. Restart Case Management Queuing Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.
14. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
15. On the RiskFort Connectivity page:
    - Ensure that the IP address or the host name of Case Management Server is correctly set in the **Server** field.
    - Ensure that the **Server Management Port** is also set to point the Case Management Server port that is open to Server Management requests.
    - Select **SSL** from the **Transport** list.
    - Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the Case Management Server root certificate.
    - Click the **Browse** button adjacent to the **Client Certificate-Key Pair in PKCS#12** field to navigate to and select the root certificate of the application server where Administration Console is deployed.
    - Enter the PKCS#12 file password in the **Client PKCS#12 Password** field.
16. Click the **Save** button.
17. Restart Case Management Queuing Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.
18. Restart Administration Console.
19. Verify that Case Management Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
    b. Open the arcotriskfortcasemgmtserverstartup.log file in a text editor.
    c. Check for the following line:
    ```
    Started listener for [Case Management Admin] [7780] [SSL]
    [srvmgrwsprotocol]
    ```
    If you located this line, then two-way SSL was set successfully.
    d. Close the file.

For Fetching Cases

Case Management Queuing Server listens to requests to fetch the next case from Administration Console by using the Case Management Queuing Server port (7779).

To set up SSL between Administration Console and Case Management Queuing Server, you must configure the Case Management Queuing Server port (7779) for SSL and provide the corresponding Server Root CA Certificate on the RiskFort Connectivity page. Additionally, if two-way SSL is required, you must upload the **Client Certificate-Key Pair in PKCS#12** file on the RiskFort Connectivity page and select the appropriate trust store on the Protocol Configuration page for this port.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 114)
- Two-Way SSL (see page 116)

One-Way SSL

To set up one-way SSL communication between Administration Console and Case Management Queuing Server for displaying the next case in the queue:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** subtab is activated.
5. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
6. Select the **Server Instance** for which you want to configure SSL communication.
7. In the **List of Protocols** section, click the **Case Management Queuing Server** link.

   The page to configure the Case Management Queuing Server protocol appears.
8. Configure the following fields:
   - Ensure that the **Protocol Status** is **Enabled**.

     If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
   - Ensure that the **Port** is set to the correct SSL port value.
   - Select **SSL** from the **Transport** list.
   - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
   - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
   - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
9. Click the **Save** button.
10. Restart Case Management Queuing Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.
11. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
12. Scroll down to the **Case Management Queuing Server Connectivity** section.
13. In the **Case Management Queuing Server Connectivity** section:

- Ensure that the IP address or the host name of Case Management Server is correctly set in the **Server** field.
- Ensure that the **Server Management Port** is also set to point the Case Management Server port that is open to console requests.
- Select **SSL** from the **Transport** list.
- Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the RiskMinder root certificate.

14. Click the **Save** button.
15. Restart Case Management Queuing Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.
16. Restart Administration Console.

Two-Way SSL

To set up two-way SSL communication between Administration Console and Case Management Server for case activities:

1. Access Administration Console in a Web browser window.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** tab is active.
5. Under **System Configuration**, click the **Trusted Certificate Authorities** link to display the Riskfort Server Trusted Certificate Authorities page.
6. Set the following information on the page:
   - In the **Name** field, enter the name for the SSL truststore.
   - Click the **Browse** button adjacent to the first **Root CAs** field and navigate to and select the root certificate of the application server where Administration Console is deployed.
7. Click the **Save** button.
8. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
9. Select the **Server Instance** for which you want to configure SSL communication.
10. In the **List of Protocols** section, click the **Case Management Queuing Server** link.

    The page to configure the Case Management Queuing Server protocol appears.
11. Configure the following fields:
    - Ensure that the **Protocol Status** is **Enabled**.

      If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
    - Ensure that the **Port** is set to the correct SSL port value.
    - Select **SSL** from the **Transport** list.
    - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
    - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
    - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
    - **Select Client Store** that you created in Step 6.
12. Click the **Save** button.
13. Restart Case Management Queuing Server:

- **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
- **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.

14. Under **System Configuration**, click the **RiskFort Connectivity** link to display the RiskFort Connectivity page.
15. On the RiskFort Connectivity page, under the **Case Management Queuing Server Connectivity** section:
    - Ensure that the IP address or the host name of Case Management Server is correctly set in the **Server** field.
    - Ensure that the **Port** is also set to point the Case Management Server port that is open to case requests.
    - Select **SSL** from the **Transport** list.
    - Click the **Browse** button adjacent to the **Server CA Root Certificate** field to navigate to and select the Case Management Server root certificate.
    - Click the **Browse** button adjacent to the **Client Certificate-Key Pair in PKCS#12** field to navigate to and select the root certificate of the application server where Administration Console is deployed.
    - Enter the PKCS#12 file password in the **Client PKCS#12 Password** field.
16. Click the **Save** button.
17. Restart Case Management Queuing Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot Case Management Queuing Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./casemanagementserver start command in the console window.
18. Restart Administration Console.
19. Verify that Case Management Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
    b. Open the arcotriskfortstartup.log file in a text editor.
    c. Check for the following line:
    ```
    Started listener for [Case Management Server] [7779] [SSL]
    [RiskFortCaseManagement]
    ```
    If you located this line, then two-way SSL was set successfully.
    d. Close the file.

Enable SSL Between Java SDK and RiskMinder Server

To enable RiskMinder Java SDK for SSL communication, you must first configure your client that accesses the SDK for SSL communication, then configure the **Native (SSL)** protocol by using Administration Console.

- One-Way SSL (see page 119)
- Two-Way SSL (see page 121)

One-Way SSL

To set up one-way SSL between the Risk Evaluation SDK and RiskMinder Server, you must first configure the RiskMinder **Native (SSL)** protocol by using Administration Console and then configure the riskfort.risk-evaluation.properties file.

To configure one-way SSL between Java SDK and RiskMinder Server:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab is active.
4. Under the **Instance Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page.
5. Select the **Server Instance** for which you want to configure the SSL.
6. In the **List of Protocols** section, click the **Native (SSL)** protocol link to display the page for configuring the protocol.
7. Configure the following fields:
   - Ensure that the **Protocol Status** is **Enabled**.

     If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
   - Ensure that the **Port** is set to the correct SSL port value.
   - Select **SSL** from the **Transport** list.
   - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
   - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select RiskMinder Server root certificate.
   - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select RiskMinder Server private key.
8. Click the **Save** button.
9. Restart RiskMinder Server:
   - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
   - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
10. Navigate to the following location:
    - Windows:
      `<install_location>\Arcot Systems\sdk\java\properties\`
    - Unix-Based Platforms:
      `<install_location>/arcot/sdk/java/properties/`

11. Open the riskfort.risk-evaluation.properties file in an editor window of your choice.

    Note: Refer to appendix, "Configuration Files and Options" in the *CA RiskMinder Installation and Deployment Guide* for more information on the riskfort.risk-evaluation.properties file.

    a. Set the following parameters:

    - TRANSPORT_TYPE= SSL (By default, this parameter is set to TCP.)
    - CA_CERT_FILE= <*absolute_path_to_Server_root_certificate_in_PEM_format*>

    For example, you can specify one of the following:

    - CA_CERT_FILE=<*install_location*>/certs/<ca_cert>.pem
    - CA_CERT_FILE=<*install_location*>\\certs\\<ca_cert>.pem

    For example, you can specify CA_CERT_FILE= <*install_location*>/certs/<ca_cert>.pem.

    Important! In the absolute path that you specify, ensure that you use \\ or / instead of \. This is because the change might not work, if you use the conventional \ that is used in Windows for specifying paths.

    b. Save the changes and close the file.

12. Restart the application server where your Java SDK is deployed.

Two-Way SSL

To set up two-way SSL between the Risk Evaluation SDK and RiskMinder Server, you must first upload the root certificates for the CAs trusted by RiskMinder, then configure the RiskMinder **Native (SSL)** protocol by using Administration Console, and finally configure the riskfort.risk-evaluation.properties file.

To configure two-way SSL between Java SDK and RiskMinder Server:

1. Enable the application server where Java SDKs are deployed for SSL communication.

   Refer to your application server vendor documentation for detailed information.
2. Log in to Administration Console using a Master Administrator account.
3. Activate the **Services and Server Configurations** tab in the main menu.
4. Ensure that the **RiskFort** tab is active.
5. Under the **Instance Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page.
6. Under **System Configuration**, click the **Trusted Certificate Authorities** link to display the Riskfort Server Trusted Certificate Authorities page.
7. Set the following information on the page:
   - In the **Name** field, enter the name for the SSL trust store.
   - Click the **Browse** button adjacent to the first **Root CAs** field and navigate to and select the root certificate of the application server where Java SDKs are deployed.
8. Click the **Save** button.
9. Under the **Instance Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page.
10. Select the **Server Instance** for which you want to configure the SSL.
11. In the **List of Protocols** section, click the **Native (SSL)** protocol link to display the page for configuring the protocol.
12. Configure the following fields:
    - Ensure that the **Protocol Status** is **Enabled**.

      If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
    - Ensure that the **Port** is set to the correct SSL port value.
    - Select **SSL** from the **Transport** list.
    - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
    - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.

- (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
- Select the **Client Store** that you created in Step 7.

13. Click the **Save** button.
14. Restart RiskMinder Server:
    - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
    - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.
15. Navigate to the following location:
    - Windows:
      <*install_location*>\Arcot Systems\sdk\java**properties**\
    - Unix-Based Platforms:
      <*install_location*>/arcot/sdk/java/**properties**/
16. Open the riskfort.risk-evaluation.properties file in an editor window of your choice.

    Note: Refer to appendix, "Configuration Files and Options" in *CA RiskMinder Installation and Deployment Guide* for more information on the riskfort.risk-evaluation.properties file.

    a. Set the following parameters:
       - TRANSPORT_TYPE= SSL (By default, this parameter is set to TCP.)
       - CA_CERT_FILE=
         <*absolute_path_to_Server_root_certificate_in_PEM_format*>

       For example, you can specify one of the following:

       - CA_CERT_FILE=<*install_location*>/certs/<ca_cert>.pem
       - CA_CERT_FILE=<*install_location*>\\certs\\<ca_cert>.pem

       For example, you can specify CA_CERT_FILE=
       <*install_location*>/certs/<ca_cert>.pem.

    Important! In the absolute path that you specify, ensure that you use \\ or / instead of \. This is because the change might not work, if you use the conventional \ that is used in Windows for specifying paths.

    b. Save the changes and close the file.
17. Restart the application server where your Java SDK is deployed.
18. Verify that RiskMinder Server is enabled for SSL communication by performing the following steps:

    a. Navigate to the following location:

b. Open the arcotriskfortstartup.log file in a text editor.

c. Check for the following line:
```
Started listener for [RiskFort Native (SSL)] [7681] [SSL]
[RiskFort]
```
If you located this line, then two-way SSL was set successfully.

d. Close the file.

Enable SSL Communication Between Risk Evaluation Web Service and RiskMinder Server

To enable RiskMinder Web services for SSL communication, you must first configure your client that accesses the Web service for SSL communication, then configure the Transaction Web Service protocol by using Administration Console.

- One-Way SSL (see page 124)
- Two-Way SSL (see page 125)

One-Way SSL

To set up one-way SSL between the Risk Evaluation Web service and RiskMinder Server:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **Instance Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page.
5. Select the **Server Instance** for which you want to configure the SSL communication.
6. In the **List of Protocols** section, click the **Transaction Web Service** link.

   The page to configure Transaction Web Service protocol appears.
7. Configure the following fields:
   - Ensure that the **Protocol Status** is **Enabled**.

     If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
   - Ensure that the **Port** is set to the correct SSL port value.
   - Select **SSL** from the **Transport** list.
   - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
   - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
   - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
8. Click the **Save** button.
9. Restart RiskMinder Server:
   - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
   - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

Two-Way SSL

To enable two-way SSL communication mode between the Risk Evaluation Web service and RiskMinder Server:

1. Log in to Administration Console as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under **System Configuration**, click the **Trusted Certificate Authorities** link to display the Riskfort Server Trusted Certificate Authorities page.
5. Set the following information on the page:
   - In the **Name** field, enter the name for the SSL truststore.
   - Click the **Browse** button adjacent to the first **Root CAs** field and navigate to and select the root certificate of the application server where your Web services client is deployed.
6. Click the **Save** button.
7. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
8. Select the **Server Instance** for which you want to configure the SSL communication.
9. In the **List of Protocols** section, click the **Transaction Web Service** link.

   The page to configure Transaction Web Service protocol appears.
10. Configure the following fields:
    - Ensure that the **Protocol Status** is **Enabled**.

      If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
    - Ensure that the **Port** is set to the correct SSL port value.
    - Select **SSL** from the **Transport** list.
    - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
    - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
    - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
    - Select the **Client Store** that you created in Step 5.
11. Click the **Save** button.
12. Restart RiskMinder Server:

- **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
- **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

13. Verify that RiskMinder Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
    b. Open the arcotriskfortstartup.log file in a text editor.
    c. Check for the following line:
    ```
    Started listener for [RiskFort Trans WS] [7778] [SSL]
    [transwsprotocol]
    ```
    If you located this line, then two-way SSL was set successfully.
    d. Close the file.

Enable SSL Communication Between Administration Web Service and RiskMinder Server

To enable Administration Web service for SSL communication, you must first configure your client that accesses the Web services for SSL communication, then configure the Administration Web Service protocol by using Administration Console.

- One-Way SSL (see page 124)
- Two-Way SSL (see page 125)

One-Way SSL

To set up one-way SSL between the Administration Web service and RiskMinder Server:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **Instance Configuration** section, click the **Protocol Configuration** link to display the Protocol Configuration page.
5. Select the **Server Instance** for which you want to configure the SSL communication.
6. In the **List of Protocols** section, click the **Administration Web Service** link.

   The page to configure Administration Web Service protocol appears.
7. Configure the following fields:
   - Ensure that the **Protocol Status** is **Enabled**.

     If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
   - Ensure that the **Port** is set to the correct SSL port value.
   - Select **SSL** from the **Transport** list.
   - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
   - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
   - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
8. Click the **Save** button.
9. Restart RiskMinder Server:
   - **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
   - **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

Two-Way SSL

To enable two-way SSL communication mode between the Administration Web Service and RiskMinder Server:

1. Log in to Administration Console as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under **System Configuration**, click the **Trusted Certificate Authorities** link to display the Riskfort Server Trusted Certificate Authorities page.
5. Set the following information on the page:
   - In the **Name** field, enter the name for the SSL truststore.
   - Click the **Browse** button adjacent to the first **Root CAs** field and navigate to and select the root certificate of the application server where your Web services client is deployed.
6. Click the **Save** button.
7. Under **Instance Configuration**, click the **Protocol Configuration** link to display the Protocol Configuration page.
8. Select the **Server Instance** for which you want to configure the SSL communication.
9. In the **List of Protocols** section, click the **Administration Web Service** link.

   The page to configure Administration Web Service protocol appears.
10. Configure the following fields:
    - Ensure that the **Protocol Status** is **Enabled**.

      If not, then select the **Change Protocol Status** option and then from the **Action** list, select **Enable**.
    - Ensure that the **Port** is set to the correct SSL port value.
    - Select **SSL** from the **Transport** list.
    - If you want to store the SSL key on an HSM, then select the **Key in HSM** option.
    - Click the **Browse** button adjacent to the **Server Certificate Chain** field to select the RiskMinder Server root certificate.
    - (*Only* if you did not select the **Key in HSM** option) Click the **Browse** button adjacent to the **Server Private Key** field to select the RiskMinder Server private key.
    - Select the **Client Store** that you created in Step 5.
11. Click the **Save** button.
12. Restart RiskMinder Server:

- **On Windows:** Click the **Start** button**,** navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Double-click **Arcot RiskFort Service** from the listed services.
- **On UNIX Platforms:** Navigate to <*install_location*>/arcot/bin/ and specify the ./riskfortserver start command in the console window.

13. Verify that RiskMinder Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
    b. Open the arcotriskfortstartup.log file in a text editor.
    c. Check for the following line:
    ```
    Started listener for [RiskFort Admin WS] [7777] [SSL]
    [aradminwsprotocol]
    ```
    If you located this line, then two-way SSL was set successfully.
    d. Close the file.

Enable One-Way SSL Between RiskMinder Components and Database

This section walks you through the steps to set up one-way SSL communication between RiskMinder components and RiskMinder database. The section covers the following topics:

- Between RiskMinder Server and Database (see page 129)
- Between Administration Console and Database (see page 131)
- Between UDS and Database (see page 131)

Between RiskMinder Server and Database

RiskMinder uses DataDirect driver to connect to the database. This section walks you through the steps to configure one-way and two-way SSL between a RiskMinder Server instance and Oracle database:

- On Windows (see page 130)
- On UNIX-Based Platforms (see page 130)

On Windows

To enable one-way SSL between RiskMinder Server and the Oracle database, perform the following configurations:

1. On the system where you have installed RiskMinder Server, open **Control Panel**, navigate to **Administrative Tools**, **Data Sources (ODBC)**, **System DSN**.
2. Select the data source that you specified during RiskMinder installation, and click **Configure**.

   The ODBC Oracle Wire Protocol Driver Setup dialog box appears.
3. In the **Encryption** section, select **1-SSL Auto** from the **Encryption Method** list.
4. Set **Truststore** to the location to the truststore file that contains a list of the valid Certificate Authorities (CAs) that are trusted by RiskMinder.
5. Specify the password for the truststore in the **Truststore Password** field.
6. Set the **Host Name in Certificate** fields to the host name of the system where your database server is installed.

   Refer to your database vendor documentation for this parameter.
7. Click **OK** to save the configurations.

On UNIX-Based Platforms

To enable SSL between RiskMinder and the database on UNIX platforms, you need to update the odbc.ini file with the required DataDirect driver information. To configure this odbc.ini file:

1. Navigate to the following location:
   `<install_location>/arcot/odbc32v60wf`
2. Open the odbc.ini file in a file editor of your choice.
3. In the [*<Database_name>* Wire Protocol] section that corresponds to the database you are using, edit the parameters required for SSL connection, as listed in the following table.

Parameter	Description
EncryptionMethod	Specifies the method the driver uses to encrypt data sent between the driver and the database server. Set this parameter to 1 to encrypt the data using SSL.
Truststore	Specifies the location of the trust store file, which contains a list of the valid Certificate Authorities (CAs) that are trusted by the client machine for SSL server authentication.

Parameter	Description
TrustStorePassword	Specifies the password required to access the trust store.
ValidateServerCertificate	Validates the security certificate of the server as part of the SSL authentication handshake. Set this parameter to 1 to validate the certificate sent by the database server.

4. Save and close the odbc.ini file.

Between Administration Console and Database

Administration Console uses Java Database Connectivity (JDBC) to connect to the database. To enable SSL between Administration Console and the database:

1. Configure the application server where Administration Console is deployed for SSL.
2. Configure the TrustStorePath.*N* and HostNameInCertificate.*N* parameters in the arcotcommon.ini file.

   Note: See "Configuration Files and Options" in *CA RiskMinder Installation and Deployment Guide* for more information on the arcotcommon.ini parameters.

Between UDS and Database

UDS also uses JDBC to connect to the database. To enable SSL between UDS and the database:

1. Configure the application server where UDS is deployed for SSL.
2. Configure the TrustStorePath.*N* and HostNameInCertificate.*N* parameters in the arcotcommon.ini file.

   Note: See "Configuration Files and Options" in *CA RiskMinder Installation and Deployment Guide* for more information on the arcotcommon.ini parameters.

Chapter 6: Understanding RiskMinder Rule Basics

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

RiskMinder uses rules to evaluate the risk associated with each transaction. These rules can be broadly categorized into the following categories:

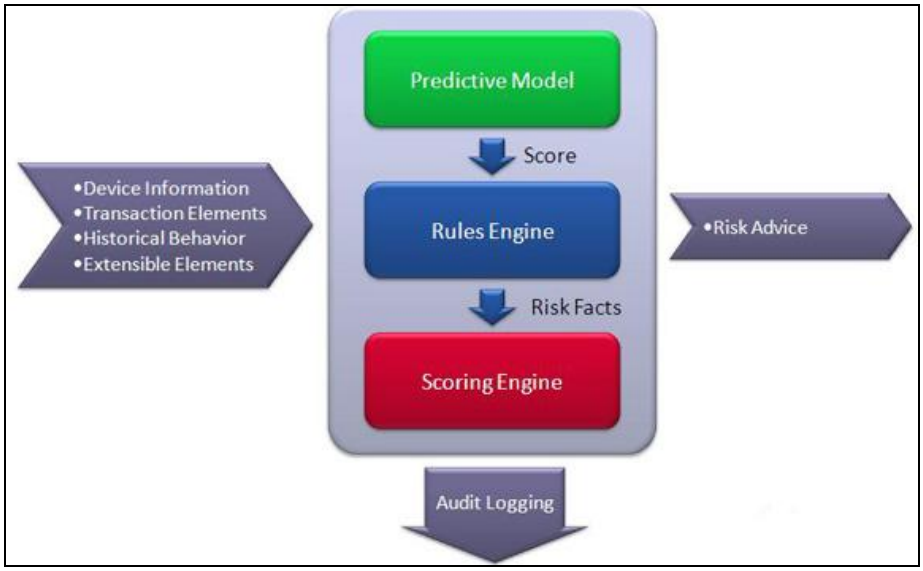
- Evaluation Rules (see page 135)
- Scoring Engine (see page 137)

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

- Ruleset: Each rule *must* belong to a Ruleset. This choice of the Ruleset determines the options that are available for a rule. For more information on working with Rulesets, see "Creating Rulesets" (see page 158).
- Rule Implementation (at global or organization level): This determines whether the rule is applicable at the global level (available as a template to organizations) or at the level of individual organizations.

  See "Managing Global Configurations" (see page 147) and "Managing Organization-Specific RiskMinder Configurations" (see page 259) for implementing rules at global and organization levels, respectively.
- Rule Type: This determines the capability and scope of the rule, and is closely associated with New Rules Added Using the Rule Builder (see page 137).

The following figure is a schematic representation of RiskMinder rules and their scoring order.



The rules are run in the following phases:

Execution Phase

RiskMinder Server does a first parse of all the rules in the active ruleset. In this phase, the Server:

1. Executes all the rules in the list in the order of execution priority.

   This execution priority is internal, and is defined by the Server.

2. Generates an individual risk score and advice for each rule it executes.

Scoring Phase

RiskMinder Server now does the second parse of the rules. In this phase, the Server:

1. Uses the result for each rule in the first parse, and parses the rules in the ruleset based on the scoring priority.

   The scoring priority is configured by the Global Administrator (GA) through Administration Console.

2. Stops the scoring at the first matched rule.
3. Returns the score and advice of the rule that matched as final.

Note: Depending on when the first rule matched, the second parse may not be run completely.

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. 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.

RiskMinder provides the following types of Evaluation rules:

- Out-of-the-Box Rules (see page 135)
- New Rules Added Using the Rule Builder (see page 137)
- Evaluation Callout (see page 137)

Out-of-the-Box Rules

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

The out-of-the-box rules can be categorized as:

- Configurable Rules (see page 135)
- Non-Configurable Rules (see page 136)

Configurable Rules

The following table lists the out-of-the-box rules that are installed and deployed by default when you install RiskMinder.

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
Exception User Check	EXCEPTION	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, RiskMinder returns a low Score and the ALLOW advice for the transactions originating from exception users.

Rule Name (Display Name)	Rule Mnemonic (Short Name)	Rule Description
Untrusted IP Check	UNTRUSTEDIP	See "Configuring Untrusted IP Addresses" (see page 205) for more information.
Negative Country Check	NEGATIVECOUNTRY	See "Configuring Negative Country List" (see page 203) for more information.
Trusted IP/Aggregator Check	TRUSTEDIP	See "Configuring Trusted IP Addresses" (see page 207) and "Configuring Trusted Aggregators" (see page 209) for more information.
Device MFP Not Match	MFPMISMATCH	Checks if the match percentage between the input signature and the corresponding stored signature is LESSER_OR_EQUAL to a specified Signature Pass Threshold and Reverse Lookup Threshold.
User Velocity Check	USERVELOCITY	See "Configuring User Velocity" (see page 194) for more information.
Device Velocity Check	DEVICEVELOCITY	See "Configuring Device Velocity" (see page 196) for more information.
Zone Hopping Check	ZONEHOPPING	See "Configuring Zone Hopping" (see page 198) for more information.

Non-Configurable Rules

In addition to the preceding configurable rules, RiskMinder also provides the following non-configurable rules:

- **Unknown User (UNKNOWNUSER)**: If the user does not exist in the RiskMinder database, then RiskMinder returns ALERT. Your application can either call the RiskMinder API to create the user in RiskMinder, or take an appropriate action.
- **Unknown DeviceID (UNKNOWNDEVICEID)**: Checks if a device (whose transaction is being evaluated) exists in the RiskMinder database. This information is used for Machine FingerPrint match.
- **User Not Associated with DeviceID (USERDEVICENOTASSOCIATED)**: Checks if a corresponding User-Device association exists.

New Rules Added Using the Rule Builder

The out-of-the-box rules in RiskMinder are generic and are configured for evaluating risk based on the rules that are applicable to all. If you need custom or industry-specific rules that are significantly different from those that RiskMinder provides out-of-the-box, then you need to deploy your own rules by using the *Rule Builder*.

Unlike the out-of-the-box rules, these rules are installed, but not deployed automatically.

See "Adding New Rules" (see page 163) for detailed information on adding new rules by using the Rule Builder wizard.

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 RiskMinder Server.

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

See "Configuring Callouts" (see page 217) for more information on working with Evaluation Callouts.

Scoring Engine

RiskMinder provides a **Scoring Engine** that accepts the input from the Evaluation Rules (see page 135) to generate the final Score and Advice.

Scoring Callout

Based on your business requirements, RiskMinder also provides you the flexibility to add your own custom scoring logic in addition to RiskMinder'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 RiskMinder's standard scoring program. The Scoring Callout will return the final risk Score, which can differ and will override the Score computed by RiskMinder's standard Scoring Engine.

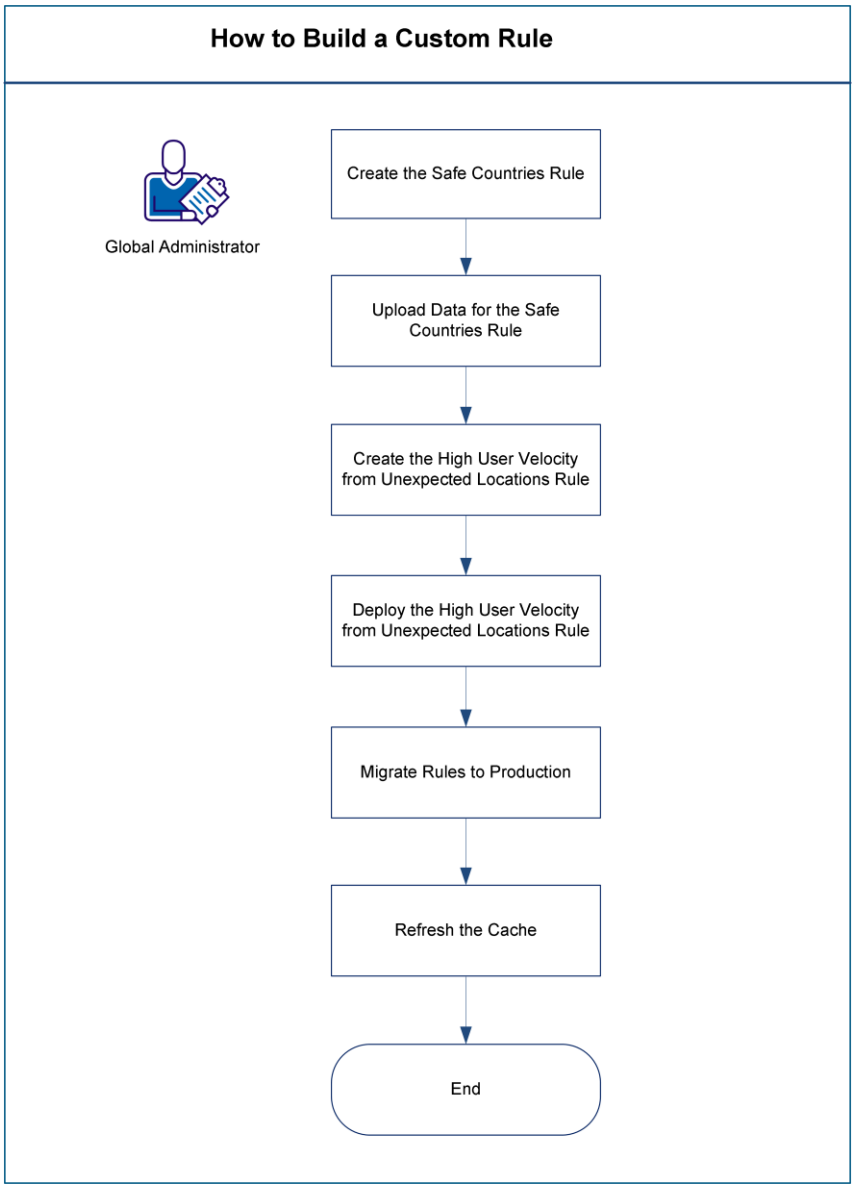
Like the Evaluation Callout (see page 137), Scoring Callout is a custom rule that executes last, after the standard RiskMinder scoring program is completed and returns a final Score and Advice.

See "Configuring Callouts" (see page 217) for more information on working with Scoring Callouts.

Chapter 7: How to Build a Custom Rule

This scenario illustrates an example of how a global administrator can build a new rule to determine transactions with a high user velocity from unusual locations. This rule is in turn dependent on another custom rule that is used to determine transactions from countries that are considered unsafe. A high user velocity indicates multiple transactions by the same user within a short (configurable) interval.

The following diagram outlines the steps that are required to create and deploy custom rules in RiskMinder.



To build a new rule, complete the following steps:

- Create the Safe Countries Rule (see page 141)
- Upload Data for the Safe Countries Rule (see page 142)
- Create the High User Velocity from Unexpected Locations Rule (see page 143)
- Deploy the High User Velocity from Unexpected Locations Rule (see page 144)
- Migrate Rules to Production (see page 145)
- Refresh the Cache (see page 146)

Create the Safe Countries Rule

To create the Safe Countries rule:

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

   The Rules and Scoring Management page opens.
4. From the Select a Ruleset list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. Click Add a New Rule.

   The RiskFort Rule Builder page opens.
6. Enter the following basic information for the rule:
   - Name: Safe Countries
   - Mnemonic: SAFECOUNTRIES
   - Description: This rule contains a list of countries that are considered to be the origin of safe transfers
7. Select Default Channel and All Actions.

   Note: Each rule must be associated with one or more Channels and Actions. By default, a rule is associated with All Channels and All Actions.
8. Build the rule fragment as follows:
   a. From the Select Data Element(s) list, select COUNTRY from GeoLocation Elements.
   b. To edit the rule that you are creating, select the IN_LIST operator from the Select Operator list.
   c. Provide an identifier for the list, such as, SAFE_COUNTRY_LIST.
   d. Click Add to add the rule fragment to the rule being developed.
9. Click Create.

   The Safe Countries rule is created.

Upload Data for the Safe Countries Rule

The Safe Countries rule that you deploy requires more data in the form of a list. This list must contain the names of countries that are considered to be the origin of safe transfers.

To upload the data for the Safe Countries rule:

1. Ensure that you are logged in as a Global Administrator.
2. Click the Services and Server Configurations tab.
3. Under the Rules Management section on the side-bar menu, click the Manage List Data and Category Mappings link.

   The Manage List Data and Category Mappings page opens.
4. From the Select Existing Ruleset list, select the ruleset for which this configuration is applicable.
5. Select the Manage List Data option.
6. From the Select List Type list, select Other Lists.
7. From the Select List drop-down list, select the list identifier that you specified while creating the corresponding list. In this case, the list identifier is SAFE_COUNTRY_LIST.

   The updated page opens.
8. In the Upload File Or Enter Data section, select the appropriate mode for writing data:
   - Append

     This option appends the data that you are uploading to a list or data set.
   - Replace

     This option overwrites the existing data in the specified list or data set.
9. Perform either of the following steps:
   - Click Browse to navigate to the data file that contains the list of entries (separated by a newline character.)
   - Type the entries in the Enter Data field, if a data file does not exist.
10. Click Upload to complete the task.

    A list of safe countries is uploaded to SAFE_COUNTRY_LIST.

Create the High User Velocity from Unexpected Locations Rule

To create the High User Velocity from Unexpected Locations rule:

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

   The Rules and Scoring Management page opens.
4. From the Select a Ruleset list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. Click Add a New Rule.

   The RiskFort Rule Builder page opens.
6. Enter the following basic information for the rule:
   - Name: High User Velocity from Unexpected Locations
   - Mnemonic: HIGH_USER_VEL_UNSAFE
   - Description: Rule to determine transactions with a high user velocity from unusual locations
7. Select the Default Channel and All Actions for which this rule is applicable.
8. From the Saved Rules list, select the out-of-the-box USERVELOCITY rule and the custom SAFECOUNTRIES rule that you created, and build your rule as follows:

   ```
   USERVELOCITY AND NOT SAFE_COUNTRIES
   ```
9. Click Create.

   The High User Velocity from Unexpected Locations rule is created.

Deploy the High User Velocity from Unexpected Locations Rule

To deploy the custom High User Velocity from Unexpected Locations rule that you created:

1. Ensure that you are logged in as a Global Administrator.
2. Click the Services and Server Configurations tab.
3. Under the Rules Management section on the side-bar menu, click the Rules and Scoring Management link.

   The Rules and Scoring Management page opens.
4. From the Select a Ruleset list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. Select the Enable option in the Rules and Scoring Management page to enable the High User Velocity from Unexpected Locations rule and the Safe Countries rule that you deployed.
6. Click Save to save your changes.

   The new rules that you deployed are not yet active and are not available to your end users. To make the new rules active, migrate them to the production environment.

Migrate Rules to Production

At any point in time, RiskMinder Servers work with Active data configurations *only*. Active data is versioned to track the changes that were made to the RiskMinder configuration data. Every time the Proposed data is migrated to production, unique data versions are created for the new set of Active configuration data.

To make the new rules active, migrate them to the production environment.

To migrate changes, follow these steps:

1. Ensure that you are logged in as a Global Administrator.
2. Select the Services and Server Configurations tab.
3. Under the Migrate to Production section on the side-bar menu, click the Migrate to Production link.

   The Migrate to Production page opens.
4. From the Select Ruleset(s) list, select the rulesets that contain the new rules.
5. Click Migrate.

   The page to confirm the action is displayed.
6. On the confirmation page, click Confirm to start the migration process.

   Note: Based on the volume of data that you are migrating to the production environment, the migration process may take a few minutes.

   After the migration is completed, a success message appears.

Now refresh the RiskMinder Server cache. This task is described in the topic that follows.

Refresh the Cache

If you made any configuration changes, refresh the cache of the affected server instances for the changes to take effect. RiskMinder now provides an *Integrated Cache Refresh* feature that enables administrators to refresh the cache of all server instances from Administration Console.

To refresh the cache:

1. Ensure that you are logged in as a Global Administrator.
2. Click the Services and Server Configurations tab.
3. Click the Administration Console option on the submenu of the tab.
4. Under the System Configuration section on the side-bar menu, click the Refresh Cache link to display the page.
5. Select one or both of the following options:
   - Select Refresh System Configuration to refresh the cache configuration of Administration Console, User Data Service, and all RiskMinder Server and Case Management Queuing Server instances.
   - Select Refresh Organization Configuration to refresh the cache configuration of all organizations in your purview.
6. Click OK.
7. Click OK in the confirmation dialog that appears.

   A message with a Request ID for the current cache refresh request is displayed.

The new rule is ready for consumption.

Chapter 8: Managing Global Configurations

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

RiskMinder configurations made at the global level are of two types:

- **System-level configurations**: These configurations are made under the **Services and Server Configurations** tab. They are applicable to *all* organizations, unless overridden for a specific organization by configuring the same under the **Organizations** tab. Any change made under the **Services and Server Configurations** tab is available to all organizations.
- **Configurations that can be used by all organizations but not automatically available to all organizations**: An example of this type of configuration is a Ruleset template created at the global level. The rulesets can optionally be used as a starting point when creating a ruleset for an organizations.

This section discusses the following:

- Organization-specific RiskMinder configurations that a GA can perform
  - Configuring Channels and Accounts Associations (see page 149)
  - Configuring RiskMinder Properties (see page 151)
  - Enabling the RiskMinder Model (see page 155)
- RiskMinder rules that a GA can set as a "template" for all current and future organizations in the system
  - Managing Global Rule Configurations (see page 156)

Logging In as a Global Administrator

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

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

To log in to Administration Console as a GA by using the basic user name-password credentials:

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

   http://<hostname>:CA Portal/arcotadmin/adminlogin.htm

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

   Note: It is recommended that you bookmark this URL to access Administration Console. Any GA, OA, or UA can use this URL to log in to Administration Console by using their User Name and Password.

   The Administrator Login page appears.
3. Enter the Organization Name that you want to log in to.

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

   The Login page appears.
5. Specify the administrator ID in the User Name field, enter the corresponding password that you received in the Password field, and click Log In.

   If you are logging in for the first time, you will be prompted to change the password.
6. Specify the New Password, Confirm Password, and then click Log In.

   You will be redirected to the login page.
7. Specify the Password again and click Log In.

   The landing page of Administration Console appears.

Logging Out of Administration Console

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

Security Recommendations While Using Administration Console

When you access Administration Console, ensure that you follow the best practices listed below:

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

Configuring Channels and Accounts Associations

RiskMinder supports risk evaluation requests coming from multiple channels. RiskMinder evaluates transactions from different channels and generates a risk score based on several factors. For example, a home banking login from USA and a 3D Secure transaction done from India in quick succession would indicate possible fraud. The following table describes the channels that are available out-of-the-box in RiskMinder.

Channel	Description
DEFAULT	Transactions that are initiated using a Web browser. This may be either a computer, smart phone, tablet, or set-top box. The default channel is the Web channel.
3D Secure	Online transactions initiated using credit card or debit card.

To assign channels and configure the account type for each channel:

Note: Configuring channels is expected to be a one-time configuration. If you want to change these settings in a production environment, contact CA Support to understand the implications. You can add a channel to your existing deployment, but removing support for a channel or account type and changing the default channel or default account type requires careful consideration.

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page appears.
6. Activate the **RiskFort Configuration** tab.
7. Under the **General RiskFort Configurations** section, click the **Assign Channels and Configure Default Account Types** link.

   The Assign Channels and Configure Default Account Types page appears.
8. Select the channels that are supported by the organization by selecting the **Select Channels to Associate** check box.
9. Select the default account type for each channel:
   - Select **User Name** as **Default Account Type** if requests from the calling application on the specific channel send the username in the Risk Evaluation APIs.
   - If requests from the calling application contain the account IDs in the user name field, select the relevant <**Default Account Type>** for the channel.
10. Select the option under **Select Default Channel** to make the channel the default one to be used for risk evaluation purposes.
11. Click **Save** to save your changes.

Configuring RiskMinder Properties

To configure RiskMinder properties:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page appears.
6. Activate the **RiskFort Configuration** tab.
7. Under the **General RiskFort Configurations** section, click the **Miscellaneous Configurations** link. The Miscellaneous Configurations page appears.
8. From the **Select Channel** list, select the channel for which you want to configure these parameters.
9. Specify values for the parameters, as described in the following table.

Parameter	Default Value	Description
User Enrollment Mode	Implicit	The mode in which the user is created in the RiskMinder database: Implicit: If you select **Implicit**, then you do not need to invoke the createUser() Web service for creating users in RiskMinder. In this case, when you call the evaluateRisk()API for a transaction, RiskMinder will automatically create users (if not already present) in RiskMinder. Explicit: If you select **Explicit**, you would need to explicitly call the createUser()Web service to create the users in RiskMinder before you can do a risk evaluation (by calling the evaluateRisk()API) for their transactions.
Base Currency Code	USD	Currency Code in which the organization does business. This parameter is used for amount-based rules and for display purposes in Case Management.

Parameter	Default Value	Description
Enable Reverse Lookup for Device Identification	No	Enable Reverse Lookup to identify the device. Select **No** if this parameter is not applicable for the channel, for example, ATM.
Use IP Address for Reverse Lookup	No	Use the IP address for reverse lookup method of device identification.
Inactivity Period Before Case is Automatically Closed (in Hours)	48	Period for which the case remains inactive before the case is closed automatically.
Number of Case Notes to Display When Working on Cases	1	Number of case notes to display when the CSR views the case on the Case Management screen.
Additional Number of Case Notes to Display on Clicking "More"	3	Number of case notes to display when the CSR clicks the **More** link under Case Notes.
Default Number of Days a User Gets Added to Exception List Through Case Management Screen	10	The number of days for which a user is added to the Exception List through the Case Management screen.
Default Transaction Display Duration (in Days)	30	Duration for which transactions are displayed to the CSR on the Case Management screen by default.
Maximum Duration for Which the Case is Exclusively Assigned to a CSR Before it is Available for Reassignment (in Seconds)	3600	The maximum duration for which a case remains exclusively assigned to a CSR viewing the case in the Console.
Number of Records on Each Page of Analyze Transactions Screen	10	Number of records to display on each page of the Analyze Transactions screen in Case Management.

Parameter	Default Value	Description
Generate Cases For Advice(s)	DENY ALERT	The RiskMinder advice(s) for which cases are to be generated. The possible values are: ■ NONE ■ DENY ■ ALERT ■ INCREASEAUTH ■ ALLOW

1. Click **Update** to save your changes.
2. Refresh the organization cache for the changes to take effect.

   See "Refreshing Organization Cache" (see page 253) for detailed information on how to do this.

Configuring RiskMinder Properties at the System Level

In addition to the organization-specific RiskMinder configurations described in Configuring RiskMinder Properties (see page 151), a GA can configure certain parameters at the system level.

To configure RiskMinder properties at the system level:

1. Ensure that you are logged in as a GA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **RiskFort** option on the submenu of the tab
4. Under **General RiskFort Configurations** section on the side-bar menu, click the **Miscellaneous Configurations** link to display the page.
5. Specify the parameters that the GA can configure at the system level, as described in the following table.

Parameter	Default Value	Description
Next Action Date Cut-Off for Including a Case in Queue Rebuild (in Seconds)	1800	The duration before a case is added to the Queue rebuild.

Parameter	Default Value	Description
Number of Records to Be Fetched in One Chunk From Database When Exporting Analyze Transactions Report (Configure this according to the maximum heap memory available on the application server.)	5000	If the number of records to export is very high, The RiskMinder application fetches datasets in chunks of small sizes to ensure that the application server does not run out of memory. If the application server has sufficient heap memory available, you can increase this value so that the RiskMinder application makes fewer number of queries to the database. This results in improved performance.
Maximum Duration for Search on Analyze Transaction Screen (in Days)	180	Maximum duration for which search is allowed in the Analyze Transaction screen.
Frequency of Automatic Queue Rebuild Schedule (in Seconds)	1800	Frequency at which the case scheduler automatically rebuilds Queues.

Note: The other parameters are described in the previous topic.

6. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Enabling the RiskMinder Model

To enable the RiskMinder Model for your organization:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page appears.
6. Activate the **RiskFort Configuration** tab.
7. Under the **Rules Management** section, click the **Model Configuration** link.
8. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The Model Configuration information appears.
9. Select **Enable Model** to enable the model.
10. Click **Save** to save your changes.
11. To make the changes active, you must migrate them to production.

    See "Migrating to Production" (see page 214) for instructions to do so.
12. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Managing Global Rule Configurations

Managing global rule configurations is a key part of RiskMinder management and optimization, and a key responsibility of GAs.

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

You can manage RiskMinder rule configurations at two levels:

- Global level, available to all organizations

  Note: Although these rules are available to all organizations, they cannot be used as-is at the organization level. For example, even if you configure a Untrusted IP Check rule at the global level, individual organizations need to configure this rule either by copying from the global rule.

- Organization level, available to individual organizations

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

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

This section discusses the configurations that GAs can set as a "template" for *all* current and future organizations in the system. These configurations include:

- Configuring Rulesets (see page 157)
- Configuring the RiskMinder Predictive Model (see page 160)
- Configuring Out-of-the-Box Rules (see page 162)
- Adding New Rules (see page 163)
- Deploying a New Rule (see page 183)
- Deploying New Device-Based Rules (see page 187)
- Editing Rule Definitions Using the Rule Builder (see page 191)

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

See "Managing Organization-Specific RiskMinder Configurations" (see page 259) for more information.

In addition to these tasks, GAs can also:

- Refresh the system and organization-level cache configuration (see "Refreshing the Cache" (see page 37) for information on how to do this.)
- Configure the account type for organizations in their purview (see "Configuring the Account Type" (see page 45) for information on how to do this.)
- Configure the basic authentication policy (see "Specifying Basic Authentication Policy Settings" (see page 49) for information on how to do this.)
- Change the profile information (see "Changing Password and Profile Information" (see page 31) for information on how to do this.)

Configuring Rulesets

This section covers the following topics:

- Understanding Rulesets (see page 157)
- Creating Rulesets (see page 158)

Understanding Rulesets

A *ruleset* is a collection of one or more RiskMinder rules ("Evaluation Rules" (see page 135) as well as "Scoring Engine" (see page 137)) that you have configured, along with their execution order and scoring priority. Each ruleset can be different from the other in terms of:

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

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

Important! RiskMinder is shipped with an out-of-the-box global ruleset called **DEFAULT**.

Creating Rulesets

Important! After you create a global ruleset as a GA, the OAs of the individual organizations must assign these rulesets to their respective organizations.

See "Assigning Rulesets" (see page 262) for more information on how to do this.

To create a ruleset:

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

   The Create Ruleset page is displayed.
5. Specify the name of the ruleset in the **Name** field.
6. In the **Advanced Option** section, if required:
   a. Select the **Copy from an Existing Ruleset** option, if you want to copy the rules configuration from an existing ruleset.
   b. Select the name of the ruleset whose configuration you want to copy from the corresponding list.

   Note: If you do not copy from an existing ruleset, the new ruleset is created with the default settings.
7. Click **Create** to create and save the new ruleset.

   The ruleset is not yet active, and not available to your end users.
8. To make the changes active, you must migrate them to production.

   See "Migrating to Production" (see page 214) for instructions to do so.

Understanding RiskMinder Scoring

For each risk evaluation request from your application, RiskMinder executes Evaluation Rules (see page 135) to generate a *Risk Score* (or *Score*). This Score is typically a value from **0** through **100** that maps to a recommended *Risk Advice* (or *Advice*.) RiskMinder then uses the Scoring Engine (see page 137) to generate the final Score and the corresponding Advice.

The following table explains the mapping between the pre-defined score value ranges and the corresponding Advice.

Note: A score of 0 is assigned to rules that must be executed but not used for scoring. If the score is set to 0, the Advice generated is SILENT.

Score Value (From)	Score Value (To)	Advice	Default Recommended Action
1	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 RiskMinder.
51	70	**INCREASEAUTH**	Perform additional authentication before proceeding any further.
71	100	**DENY**	Deny the transaction.

You can configure RiskMinder scoring to meet your business requirements by using the Rules and Scoring Management page. For more information, see "Configuring Out-of-the-Box Rules" (see page 162).

Configuring the RiskMinder Predictive Model

Note: The RiskMinder Predictive Model is an optional component. If you are interested in using a predictive model, contact your Account Manager and initiate a statement of work.

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

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

You can configure the URL and timeout parameters for the RiskMinder Predictive Model using Administration Console.

To configure the RiskMinder Predictive Model:

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

   The Model Configuration page appears.
5. In the **Proposed Value** column, specify the parameters as described in the following table.

Parameter	Description
Predictive Model URL (primary)	The primary URL of the RiskMinder Predictive Model.
Predictive Model URL (backup)	The backup URL of the RiskMinder Predictive Model.
Connection Timeout (in milliseconds)	The time in which connection between RiskMinder Server and the Predictive Model will expire.
Read Timeout (in milliseconds)	The time in which RiskMinder Server expects a response back from the Predictive Model.
Minimum Connections	The minimum number of connections in the connection pool to connect to the Model Server.

Parameter	Description
Maximum Connections	The maximum number of connections in the connection pool to connect to the Model Server.

6. Click **Upload Model Configuration** to save the changes.

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

7. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring Out-of-the-Box Rules

Use the Rule Configuration page for:

- Enabling or disabling the out-of-the-box rules
- Configuring the risk score and priority of the out-of-the-box rules

To enable or disable rules and to configure the risk score and priority of the out-of-the-box rules:

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

   The Rules and Scoring Configuration page appears.
5. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
6. For each rule, in the **PROPOSED** column of the displayed table:
   a. Select (to enable the rule) or clear (to disable the rule) the **Enable** option.
   b. Specify the required **Risk Score**.
   c. Select a priority for the rule from the **Priority** list.
7. In the **PROPOSED** column for **Default Score** (the second table on the page), specify the required Risk Score.

   Note: RiskMinder uses this value to generate the final Risk Score and Advice if none of the rules in the preceding table match. The minimum value that you can set for the default score is 1.
8. Click **Save** to save the changes you made on this screen.

   The changes are not yet active and are not available to your end users.
9. To make the changes active, you must migrate them to production.

   See "Migrating to Production" (see page 214) for instructions to do so.
10. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Adding New Rules

The out-of-the-box Evaluation Rules (see page 135) in RiskMinder are generic and are configured to evaluate risk for typical transactions. You can tweak the scores and priority of the default rules or create Whitelists and Blacklists to improve the results, but this might not be sufficient in all cases. In such cases, you can add new rules that are significantly different from those that RiskMinder provides out-of-the-box.

You can use the Rule Builder to combine the out-of-the-box rules (such as Velocity rules) or your uploaded lists with transaction, device, and geolocation elements, mathematical operators, and boolean functions to identify fraudulent transactions.

Data Elements and Operators Used for Building New Rules

You need the following elements to build a new rule:

- Data Elements
- Operators

Data Elements

Depending on the rule that you want to create, you can select from the following data elements:

- **Transaction Elements**: Enable you to create a rule to identify suspicious transaction patterns on all channels.
- **Device Elements**: Enable you to create a rule to identify risk associated with a particular device.
- **Geolocation Elements**: Enable you to create a rule to analyze the user's geolocation data from where the transaction was performed.
- **Model Elements**: Enable you to create a rule to analyze a transaction based on the Model score.
- **Custom Elements**: Enable you to create your own data element, which is not available in the list of pre-configured data elements. For a list of element names that you can use for custom elements, see "RiskMinder Rule Tags" (see page 385).

Operators

Operators that you use to create rules can be grouped into the following categories:

- **Expression**: These operators are used to combine rule fragments to build a rule. Possible operators include AND, OR, NOT, (, and) operators.
- **Match Type:** These operators are used by the IN_CATEGORY and IN_LIST operators. Possible operators include the following:
  - EXACT: If the list value matches the input value exactly, then the rule is triggered.
  - PARTIAL: If any of the values in the list is a partial subset of the input value, then the rule is triggered
- **LookUp Type:** Possible operators include IN_LIST,IN_TRUSTED_LIST, and IN_NEGATIVE_LIST.
- **Operator:** These operators are used for numeric comparison of data elements. Possible operators include EQUAL_TO (=), NOT_EQUAL_TO (!=), GREATER_OR_EQUAL (>=), LESS_OR_EQUAL (<=), GREATER_THAN (>), and LESS_THAN (<).

The following table describes the transaction elements and the corresponding operators.

Data Element	When to Use	Operator Description
ACTION	If your rule needs to track whether one or more pre-defined actions is available in a list or performed during a particular duration.	■ IN_LIST:Checks whether the action performed is available in a simple look-up list. Only exact match is allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ VELOCITY:Checks whether the frequency of transactions of the specified set of actions have met or exceeded a pre-defined threshold and returns True if this condition is met. This rule is useful to detect situations where a prior password change makes the current transaction risky. For example, to check for a money transfer preceded by a password reset in the last 24 hours, you must set this rule **Greater Or Equal To** 1 **In last** 24 Hours for the FORGOT_PWD action in the **For Set of Actions** list. ■ IN_CATEGORY: Checks for the action performed in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
USERNAME	If your rule needs to check whether the transaction was performed by a particular user.	■ IN_LIST: Checks whether the user is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ VELOCITY: Checks whether the number of transactions for a particular user exceeds the limits set by the specified duration and frequency. ■ ZONE_HOP: Checks for transactions that originate from the same user from large distances within a short interval. ■ UNKNOWN: Checks whether the user is already registered in the RiskMinder database. ■ IN_CATEGORY: Checks for the user in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
CURRENTTIME	If your rule needs to identify suspicious transaction patterns based on the time the transaction was performed.	■ Compares the **CURRENTTIME** when the transaction was performed with the specified **Time** by using the following operators: – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_LIST: Checks whether **CURRENTTIME** is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for **CURRENTTIME** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** The format of **CURRENTTIME** is HHMM.

Data Element	When to Use	Operator Description
DATE	If your rule needs to identify suspicious transaction patterns based on the date the transaction was performed.	■ IN_LIST: Checks whether **DATE** is in a simple look-up list. Only exact match is allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ Compares the transaction **DATE** with the specified **Date** by using the following operators: – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY: Checks for **DATE** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** The format of **DATE** is YYYYMMDD.
DAYOFMONTH	If your rule needs to identify suspicious transaction patterns based on the day of the month when the transaction was performed.	■ IN_LIST: Checks whether **DAYOFMONTH** is in a simple look-up list. Only exact match is allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ Compares the **DAYOFMONTH** when the transaction was performed with the selected **Day of Month** by using the following operators: – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY: Checks for **DAYOFMONTH** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note: DAYOFMONTH** is a 2-digit number where 01=January, 02=February, and so on.

Data Element	When to Use	Operator Description
DAYOFWEEK	If your rule needs to identify suspicious transaction patterns based on the day of the week when the transaction was performed.	■ IN_LIST: Checks whether **DAYOFWEEK** is in a simple look-up list. Only exact match is allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for **DAYOFWEEK** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** Permitted values for **DAYOFWEEK** are SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, and SATURDAY.
MONTH	If your rule needs to identify suspicious transaction patterns based on the month the transaction was performed.	■ IN_LIST: Checks whether the transaction **MONTH** is in a simple look-up list. Only exact match is allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ Compares the transaction **MONTH** with the specified **Month** using the following operators: – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY: Checks for **MONTH** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** The format of **MONTH** is MM.

Data Element	When to Use	Operator Description
YEAR	If your rule needs to identify suspicious transaction patterns based on the year the transaction was performed.	■ IN_LIST: Checks whether the transaction **YEAR** is in a simple look-up list. Only exact match is allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ Compares the transaction **YEAR** with the specified **Year** using the following operators: – EQUAL_TO – NOT_EQUAL_TO \xE2\x80\x93 GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY: Checks for **YEAR** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** The format of **YEAR** is YYYY.

The following table describes the transaction elements that are specific to the 3D Secure channel.

Data Element	When to Use	Operator Description
ACQ_BIN	If your rule needs to check the acquirer bin of the merchant where the transaction was made.	■ IN_LIST: Checks whether the Acquirer BIN is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for Acquirer BIN in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
AMOUNT	If your rule needs to track transactions against a threshold amount in the specified currency. You can configure your rule to support automatic currency conversion. If this is enabled, then you need to only specify the threshold amount in your base currency. You may specify thresholds in additional currencies where you want to override the automatic conversion. For more information on the currency conversion table, see appendix, "Currency Conversion" (see page 419).	■ Compares the transaction **AMOUNT** with the specified amount using the following operators: – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_LIST: Checks whether the **AMOUNT** is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the **AMOUNT** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
CURRCODE	If your rule needs to check the 3-digit numeric code used for the transaction.	■ IN_LIST: Checks whether the currency code is in a simple look-up list. Only exact match is allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the currency code in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
MERCHANT_ID	If your rule needs to identify suspicious transaction patterns based on the unique identifier of the merchant involved in the transaction.	■ IN_LIST: Checks whether merchant ID is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the merchant ID in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
MERCHANT_NAME	If your rule needs to identify suspicious transaction patterns based on the name of the merchant involved in the transaction.	■ IN_LIST: Checks whether merchant name is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the merchant name in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
MERCHANT_URL	If your rule needs to identify suspicious transaction patterns based on the URL of the merchant involved in the transaction.	■ IN_LIST: Checks whether the merchant URL is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the merchant URL in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
MERCH_CAT	If your rule needs to identify suspicious transaction patterns based on the category of the merchant involved in the transaction.	■ IN_LIST: Checks whether merchant category is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the merchant category in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
MERCH_COUN	If your rule needs to identify suspicious transaction patterns based on the country code of the merchant where the purchase is being made. MERCH_COUN is 3-digit ISO country code.	■ IN_LIST: Checks whether the merchant country is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the merchant country in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Data Element	When to Use	Operator Description
PREVTXNDATA	If your rule wants to check whether the previous transaction matches any of the selected actions in the specified number of hours. The rule returns True if a previous transaction type was the same as the selected type for this user in the specified time frame.	CHECK: Checks whether the type of the previous transaction performed in the specified duration for the given user matches one or more of the selected actions. The transaction types are: ■ **REGULAR**: Regular purchase transaction. ■ **ATTEMPTS**: Attempts transaction (user is not enrolled and the bank is permitted to notify the merchant that the bank attempted to authenticate the user). ■ **AE_WITH_PWD**: Auto enrollment where all card holders have a valid password. ■ **AE_WITHOUT_PWD**: Auto enrollment where some of the card holders may have empty passwords. ■ **FORGOT_PWD**: Forgot password transaction. ■ **SEC_CH**: Secondary Cardholder Addition (An additional card holder (username/password) was added to an existing card number). ■ **FORGOT_PWD_MULTI_CH**: Forgot password transaction in a multiple cardholder scenario. ■ **FORGOT_PWD_SINGLE_CH**: Forgot password transaction in a single cardholder scenario (This is the same as **FORGOT_PWD**). ■ **ABRIDGED_ADS**: Activation during shopping with a temporary password. ■ **SEC_CH_ABRIDGED**: Secondary cardholder through abridged registration. ■ **UNKNOWN**: Unknown transaction type (this is an exceptional situation).

The following table describes the Device elements and the corresponding operators.

Data Element	When to Use	Operator Description
BROWSER	If your rule needs to check the browser from which the transaction originated.	■ IN_LIST: Checks whether the browser name is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the browser name in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** Supported browsers are Mobile Safari, Android Webkit, Microsoft Internet Explorer, Firefox, Epiphany, K-Meleon, Konqueror, Minimo, Mozilla, SeaMonkey, Netscape, NetPositive, Novarra, OmniWeb, Opera, Safari, Camino, Shiira, Lynx, w3m, Chrome, CrMo, CriOS, Avant Browser, PSP, ELinks, Links, and OffByOne.
DEVICEID	If your rule needs to identify suspicious transaction patterns based on the ID of the device involved in the transaction.	■ VELOCITY: Checks whether the number of transactions performed by one or more users from a specific device exceeds the limits set by the duration and frequency. ■ UNKNOWN: Checks whether the device is a recognized device. ■ IN_LIST: Checks whether the Device ID is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the Device ID in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. ■ VELOCITY_DISTINCT_USER: Counts the number of *n* distinct users who have done a transaction in the configured duration from the specific device. For more information, see "Creating the Device User Velocity Rule" (see page 188).

Data Element	When to Use	Operator Description
DEVICETYPE	If your rule needs to check for the type of device involved in the transaction.	■ IN_LIST: Checks whether the device type is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the device type in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** Supported device types are PC, Mac, iPad, iPhone, Kindle, Android, Linux, BlackBerry, Nokia, iPod, PlayBook, Web OS, HP Tablet, Sony, PlayStation, and Nintendo Wii.
MFPMATCHPERCENT	If your rule needs to check for the Machine FingerPrint match.	Checks if the match percentage between the input device signature and the corresponding stored device signature is **LESSER_OR_EQUAL** to the following thresholds: ■ Signature Match Threshold: Threshold against which match percentage is checked in cases where the transaction has a valid Device ID and the input signature is matched against the signature of the previous transaction. ■ Reverse Lookup Threshold: Threshold against which match percentage is checked in cases where the Device ID is obtained by matching the input device signature against the device signatures that were successfully associated with the user.

Data Element	When to Use	Operator Description
OS	If your rule needs to check for the operating system used by the device involved in the transaction.	■ IN_LIST: Checks whether the operating system is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the operating system value in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. **Note:** Supported OSs are Windows 98, Windows 95, Windows NT 4.0, Windows NT 3.51,Windows NT, Windows CE, Windows, PPC Mac OS X Mach-O, PPC Mac OS X, Intel Mac OS X, PPC Mac OS, Intel Mac OS, Mac OS, Macintosh, Linux, FreeBSD, NetBSD, OpenBSD, Debian, Gentoo, Red Hat Linux, SUSE, CentOS, Fedora, Mandriva, PCLinuxOS, Ubuntu, OS/2, SunOS, PalmOS, Symbian, Darwin, J2ME/MIDP, PSP, iOS, and Android.

The following table describes the Geolocation elements and the corresponding operators.

Data Element	When to Use	Operator Description
CITY	If your rule needs to check for the city from which the transaction originated.	■ IN_LIST: Checks whether the city of origin is in a simple look-up list. Exact and partial matches are allowed. ■ IN_CATEGORY: Checks for the city of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202).

Data Element	When to Use	Operator Description
CLIENTIPADDRESS	If your rule needs to check for the client IP address used to perform the transaction.	■ IN_TRUSTED_LIST: Checks whether the IP address of the client is in a pre-defined list of trusted IP addresses. ■ IN_LIST: Checks whether the IP address is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ VELOCITY: Checks whether the number of transactions from this IP address exceeds the limits set by the duration and frequency. ■ IN_NEGATIVE_LIST: Checks for anonymizing proxies. ■ IN_CATEGORY: Checks for the IP address in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.
CONNECTIONTYPE	If your rule needs to check the type of connection used to perform the transaction. **CONNECTIONTYPE** indicates the type of connection to the Internet provider.	■ IN_LIST: Checks whether the **CONNECTIONTYPE** is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for **CONNECTIONTYPE** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. For a list of possible values, see "Connection Type" (see page 408).

Data Element	When to Use	Operator Description
CONTINENT	If your rule needs to check for the continent from which the transaction originated.	■ IN_LIST: Checks whether the continent from which the transaction originated is in a simple look-up list. Exact and partial matches are allowed. RiskMinder derives the country information based on the input IP address. ■ IN_CATEGORY: Checks for the continent from which the transaction originated in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). For a list of continents, see "Continent" (see page 410).
COUNTRY	If your rule needs to check for the country from which the transaction originated.	■ IN_NEGATIVE_LIST: Checks whether the country of origin is in a pre-defined list of "negative" countries. ■ IN_LIST: Checks whether the country of origin is in a simple look-up list. Exact and partial matches are allowed. RiskMinder derives the country information based on the input IP address. ■ IN_CATEGORY: Checks for the country of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202).

Data Element	When to Use	Operator Description
IP_ROUTINGTYPE	If your rule needs to check for the IP routing type of the connection used to perform the transaction. **IP_ROUTINGTYPE** is an attribute of the IP address that helps assess the accuracy of the location.	■ IN_LIST: Checks whether the **IP_ROUTINGTYPE** is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for **IP_ROUTINGTYPE** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. For a list of possible values, see "IP Routing Type" (see page 407) in appendix.
LINESPEED	If your rule needs to check for the speed of the user's internet connection used to perform the transaction.	■ IN_LIST: Checks whether the **LINESPEED** is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for **LINESPEED** in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. For a list of possible values, see "Line Speed" (see page 409).

Data Element	When to Use	Operator Description
REGION	If your rule needs to check for the state from which the transaction originated.	■ IN_LIST: Checks whether the state of origin is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the state of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). For a list of possible values, see "Region" (see page 410).
STATE	If your rule needs to check for the state from which the transaction originated.	■ IN_LIST: Checks whether the state of origin is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the state of origin in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed. You can upload data to the data list and manage category mappings in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202).

The following table describes the Model Element and the corresponding operators.

Data Element	When to Use	Operator Description
MODEL_SCORE	If your rule needs to check for the resulting score from the model evaluation	■ Compares the model score with the specified value using the following operators: – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_LIST: Checks whether the model score is in a simple look-up list. Exact and partial matches are allowed. You can view the list and upload data to this list in the Manage List Data and Category Mappings page. For instructions to do so, see Uploading Rule List Data (see page 202). ■ IN_CATEGORY: Checks for the model score in a table in the mapping data set, and then compares the associated derived value of the input in a list data set. Exact and partial matches are allowed.

Examples of Using New Rules

The following subsections illustrate how you can combine out-of-the-box RiskMinder rules and your rules to define custom combination rules by using multiple factors and conditions:

- High Amount Check
- High User Velocity from Unexpected Locations
- High Device Velocity from Unexpected Locations
- Wire Transfers from Unexpected Locations

Note: The rule (for example, SAFE_COUNTRIES) that you see in the following examples represent a simple list rule that uses a list of countries considered to be the origin of safe transfers.

High Amount Check

Consider the following details for an AMOUNT_CHECK rule that must check for transaction amounts more than $500:

- **Rule Mnemonic:** HIGHAMTCHK
- **Rule Display Name:** High Amount Check
- **Description:** This rule checks for high transaction amounts that exceed $500.
- **Amount:** 500

This example rule performs the following:

1. Parses the AdditionalInput string (say Amount=750) that is passed in the evaluateRisk() API call by the tag named Amount, and extract the value of this tag in a variable, say ActualAmount.

   Note: Refer to the Javadocs for details on parsing the AdditionalInput elements.

2. Extracts the parameter value (500) for the rule, and store it in a variable, say ParameterAmount.
3. Returns Matched because ActualAmount(750), in this case, is greater than ParameterAmount (500).

High User Velocity from Unexpected Locations

Consider that the SAFE_COUNTRIES refers to a simple list rule (where some of the elements are US,CA, UK, DE), then you can define a new rule to determine transactions with high User Velocity from unusual locations as:

```
USERVELOCITY AND NOT SAFE_COUNTRIES
```

High Device Velocity from Unexpected Locations

Similar to "High User Velocity from Unexpected Locations", you can define a new rule to determine transactions with high Device Velocity from unusual locations as:
`DEVICEVELOCITY AND NOT SAFE_COUNTRIES`

Wire Transfers from Unexpected Locations

Consider that you have created a rule called HIGHAMTCHK (as discussed in "High Amount Check".) Also, if the SAFE_COUNTRIES rule uses a list of countries considered to be origin of safe transfers, then you can define a rule to track low-value or high-amount wire transfers from unusual locations as:
`(HIGHAMTCHK OR Amount < 20) AND NOT SAFE_COUNTRIES`

Deploying a New Rule

To deploy a new rule:

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

   The Rules and Scoring Management page appears.
4. From the **Select a Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. Click **Add a New Rule**.

   The RiskFort Rule Builder page is displayed.
6. Enter the basic information for the rule, as described in the following table.

Field	Description
Name	The display name for the rule that you want to create.
Mnemonic	A short name for the rule that is used for logging purposes and in APIs. The maximum length of the mnemonic is 15 characters and no spaces are allowed.
Description	A short description of the rule being created.

7. Select the **Channels** and **Actions** for which this rule is applicable.

   If you want to select all the channels and all the actions, select the **All Channels** and **All Actions** check boxes.

   Note: Each rule must be associated with one or more Channels and Actions. By default, a rule is associated with **All Channels** and **All Actions**.

8. Build the rule fragment, as follows:

   a. From the **Select Data Element(s)** list, select from the following elements:

      - Transaction
      - Device
      - Geolocation
      - Model
      - Custom

      For more information on elements, see "Data Elements".

   b. Select the operator from the **Select Operator** list to edit the rule that you are creating.

      For more information on operators, see "Operators".

   c. Click **Add** to add the rule fragment to the **Rule being developed** area.

9. Build your complete rule by using the available logical operators, your rule fragment, and the rules in the **Saved Rules** list.

10. Click **Create** to create your rule.

11. Select **Enable** in the Rules and Scoring Management page to enable the new rule that you deployed.

    The new rule you just deployed is not yet active and is not available to your end users.

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

    See "Migrating to Production" (see page 214) for instructions to do so.

13. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Deploying a New Rule Without Scoring

In some cases, you might want to just observe how a rule runs, but not want to include the rule score in the final advice. This release of RiskMinder allows you to define a new rule and observe how it runs without enabling it for scoring. To deploy a new rule without scoring:

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

   The Rules and Scoring Management page appears.
4. From the **Select a Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. Click **Add a New Rule**.

   The RiskFort Rule Builder page is displayed.
6. Enter the basic information for the rule, as described in the following table.

Field	Description
Name	The display name for the rule that you want to create.
Mnemonic	A short name for the rule that is used for logging purposes and in APIs. The maximum length of the mnemonic is 15 characters and no spaces are allowed.
Description	A short description of the rule being created.

7. Select the **Channels** and **Actions** for which this rule is applicable.

   If you want to select all the channels and all the actions, select the **All Channels** and **All Actions** check boxes.

   Note: Each rule must be associated with one or more Channels and Actions. By default, a rule is associated with **All Channels** and **All Actions**.

8. Build the rule fragment, as follows:

   a. From the **Select Data Element(s)** list, select from the following elements:

      - Transaction
      - Device
      - Geolocation
      - Model
      - Custom

      For more information on elements, see "Data Elements".

   b. Select the operator from the **Select Operator** list to edit the rule that you are creating.

      For more information on operators, see "Operators".

   c. Click **Add** to add the rule fragment to the **Rule being developed** area.

9. Build your complete rule by using the available logical operators, your rule fragment, and the rules in the **Saved Rules** list.

10. Click **Create** to create your rule.

11. Select **Enable** in the Rules and Scoring Management page to enable the new rule that you deployed.

    The new rule you just deployed is not yet active and is not available to your end users.

12. Specify the **Risk Score** as 0.

    Setting the risk score to 0 ensures that this rule is not taken into account for risk scoring.

13. From the **Priority** list, set the priority for this rule to 1.

    Setting the rule priority to 1 ensures that this is the first rule to be executed.

14. Click Save to save your changes.

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

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

    See "Migrating to Production" (see page 214) for instructions to do so.

16. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Deploying New Device-Based Rules

This release of RiskMinder allows you to create the following new rules based on Device-User associations:

- Device User Velocity
- Device User Maturity

Creating the Device User Velocity Rule

The existing Device Velocity Check rule checks if there are frequent transactions by one or more users from a particular device, exceeding a defined velocity. This can result in inaccurate results in cases where a single device is shared by many users. The new *Device User Velocity* rule allows a device to be used by *n* distinct users in any configured duration. If the device is used by more than *n* distinct users in the configured duration, then it indicates fraudulent activity.

It is based on the following parameters:

- **Number of Distinct Users Allowed Per Device**

  Denotes the number of distinct users performing transactions using a specified device, irrespective of whether the risk evaluation resulted in success or failure.

  The default value for this parameter is **5**.

- **Time Interval**

  Denotes the time period in which the number of transactions are tracked.

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

- **Unit for Time Interval**

  Denotes the unit in which the time period is measured.

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

For example, consider a configuration of 5 transactions per device in 60 minutes. This rule is not triggered when User1 performs five transactions per hour from Device1. But if there are transactions from five different users using Device1 in one hour, then this rule is triggered.

To create the Device User Velocity rule:

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

   The Rules and Scoring Management page appears.
4. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. Click **Add a New Rule**.

   The RiskFort Rule Builder page appears.
6. Enter the **Name**, **Mnemonic**, and **Description** of the rule that you want to create.
7. Select the **Channels** and **Actions** for which this rule is applicable.

8. Build the rule fragment, as follows:
   a. From the **Device Elements** list, select **DEVICEID**.
   b. Select **VELOCITY_DISTINCT_USER** from the **Select Operator** list.
   c. Specify the number of distinct users performing transactions from the device in the **Greater than** field.
   d. Specify the time interval.

      This value denotes the maximum number of transactions (within the specified time interval) that is considered safe for a device for *n* distinct users. If the actual number of transactions within the specified time exceeds this number, then RiskMinder tracks the transaction as a risk, which results in the matching of the Device User Velocity rule.
   e. Select the unit for the time interval from the drop-down list.
   f. Click **Add** to build the rule fragment.
9. Click **Create** at the bottom of the Rule Builder page to create the rule.

   The changes are not yet active and are not available to your end users.
10. To make the changes active, you must migrate them to production.

    See "Migrating to Production" (see page 214) for instructions to do so.
11. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Creating the Device User Maturity Rule

The *User Not Associated with DeviceID* rule evaluates transactions by checking the association between the user and the device, irrespective of the time the association was created. If the user-device association exists, then the transactions receive a low risk score. There might be cases where fraudsters can reset a user's password and associate themselves with the device. In such cases, evaluating the transaction based only on the User-Device association might not be sufficient to rule out fraudulent activity.

The *Device User Maturity* rule enables setting a level of trust in the device. For example, a User-Device association that has existed for a month, assuming that there has been no fraudulent activity identified for that user or device, should be more trusted than a User-Device association that has been established recently.

It is based on the following parameters:

- **Number of Successful Transactions per User-Device Association**

  Denotes the number of successful transactions identified by RiskMinder for a specified User-Device association.

- **First Successful Transaction**

  Denotes the time (in days) before which the first successful transaction was identified.

These parameters determine the strength of the User-Device association. The Device User Maturity rule returns True if the user has used the device for at least the specified number of days and the number of successful transactions is greater than or equal to the configured value.

To create the Device User Maturity rule:

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

   The Rules and Scoring Management page appears.
4. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. Click **Add a New Rule**.

   The RiskFort Rule Builder page appears.
6. Enter the **Name**, **Mnemonic**, and **Description** of the rule that you want to create.
7. Select the **Channels** and **Actions** for which this rule is applicable.

8. Build the rule fragment, as follows:
   a. From the **Transaction Elements** list, select **USERNAME**.
   b. Hold the **CTRL** key, and select **DEVICEID** from the **Device Elements** list.
   c. Select **MATURITY** from the **Select Operator** list.
   d. Specify the number of successful transactions.
   e. Specify the number of days before which the first successful transaction took place.
   f. Click **Add** to build the rule fragment.
9. Click **Create** at the bottom of the Rule Builder page to create the rule.

   The changes are not yet active and are not available to your end users.
10. To make the changes active, you must migrate them to production.

    See "Migrating to Production" (see page 214) for instructions to do so.
11. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Editing Rule Definitions Using the Rule Builder

This section describes how you can use the Rule Builder to make changes to the following rule definitions:

- Untrusted IP Check
- User Velocity Check
- Device Velocity Check
- Zone Hopping Check
- Device MFP Not Match

Configuring Untrusted IP Types

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

- **Negative**

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

  Important! Use this option, if you manually configured an IP addresses as negative, as discussed in "Configuring Untrusted IP Addresses" (see page 205).

- **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 currently available.

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

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

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

   The Rules and Scoring Management page appears.
4. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.

5. In the **RULENAME** column, click the **Untrusted IP Check** link.

   The RiskFort Rule Builder page appears.

6. In the **Negative IP Types Configuration** section, select the applicable types of negative IP address categories, and click **Update**.

7. Click **Update** at the bottom of the Rule Builder page to save the changes.

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

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

   See "Migrating to Production" (see page 214) for instructions to do so.

9. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring User Velocity

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

- Number of Risk Evaluations per User

  Denotes the number of transactions (**N**) performed by RiskMinder for a specified user, irrespective of the Advice or Risk Score.

  The default value for this parameter is **5**.

- Time Interval

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

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

- Unit for Time Interval

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

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

To configure the User Velocity Check rule:

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

   The Rules and Scoring Management page appears.
4. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. In the **RULENAME** column, click the **User Velocity Check** link.

   The RiskFort Rule Builder page appears.
6. Specify a value for the number of risk evaluations per user in the **Greater than** field.
7. Specify the time interval.

   This value denotes the maximum number of transactions (within the specified time interval) that is considered safe for a user. If the actual number of transactions within the specified time exceeds this number, then RiskMinder will track it as a risk, which will result in the matching of the User Velocity rule.
8. Select the unit for the time interval from the drop-down list.
9. Click **Update** to build the rule fragment.
10. Click **Update** at the bottom of the Rule Builder page to save the changes.

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

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

    See "Migrating to Production" (see page 214) for instructions to do so.

12. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring Device Velocity

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

- **Number of Risk Evaluations per Device**

  Denotes the number of transaction (**M**) performed by RiskMinder for a specified device, irrespective of 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 tracked.

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

- **Unit for Time Interval**

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

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

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

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

   The Rules and Scoring Management page appears.
4. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. In the **RULENAME** column, click the **Device Velocity Check** link.

   The RiskFort Rule Builder page appears.
6. Specify the number of risk evaluations per device in the **Greater than** field.
7. Specify the time interval.

   This value denotes the maximum number of transactions (within the specified time interval) that is considered safe for a device. If the actual number of transactions within the specified time exceeds this number, then RiskMinder tracks the transaction as a risk, which results in the matching of the Device Velocity rule.
8. Select the unit for the time interval from the drop-down list.
9. Click **Update** to build the rule fragment.
10. Click **Update** at the bottom of the Rule Builder page to save the changes.

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

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

    See "Migrating to Production" (see page 214) for instructions to do so.

12. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring Zone Hopping

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

The Zone Hopping Check rule is based on the following parameters:

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

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

  If the speed at which a user appears to have moved (in the time frame between two successive transactions) exceeds this pre-configured threshold speed (S), then RiskMinder 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 the **Maximum Speed at which a User can Travel** field in the RiskFort Rule Builder page.

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

  Sometimes, multiple users (for example, husband and wife) can use the same user name because they might be located in different zones. In such cases, RiskMinder 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 RiskMinder will not mark these transactions as risky.

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

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

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

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

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

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

   The Rules and Scoring Management page appears.

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

   The configuration information for the specified ruleset appears.

5. In the **RULENAME** column, click the **Zone Hopping Check** link.

   The RiskFort Rule Builder page appears.

6. Specify a value for the **Maximum Speed at Which the User Can Travel** parameter.
7. Specify a value for the **Maximum Number of Users Sharing the Same User ID** parameter.
8. Specify a value for the **Maximum Distance Tolerance for IP Address Location** parameter.
9. Click **Update**.
10. Click **Update** at the bottom of the Rule Builder page to save the changes.

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

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

    Refer to "Migrating to Production" (see page 214) for instructions to do so.

12. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring Machine FingerPrint (MFP) Match Percentage

The *Device MFP Not Match* rule checks if the match percentage between the input device signature and the corresponding stored device signature is lesser than or equal to a specified Signature Pass Threshold and Reverse Lookup Threshold.

To configure the Device MFP Not Match rule:

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

   The Rules and Scoring Management page appears.
4. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
5. In the **RULENAME** column, click the **Device MFP Not Match** link.

   The RiskFort Rule Builder page appears.
6. Enter a value for the **Signature Match Threshold** and **Reverse Lookup Threshold**, and click **Update**.
7. Click **Update** at the bottom of the Rule Builder page to save the changes.

   The changes are not yet active and are not available to your end users.
8. To make the changes active, you must migrate them to production.

   Refer to "Migrating to Production" (see page 214) for instructions to do so.

Deleting a Rule

Important! You can delete only the new rules that you have created and deployed. You cannot delete the out-of-the-box rules shipped with RiskMinder.

To delete a deployed rule, perform the following steps:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under **Select Organizations to Modify**, click the link with the organization's name for which you want to delete the rule.
5. Click the **RiskFort Configuration** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Rules and Scoring Management** link.

   The Rules and Scoring Management page appears.
7. From the **Select the Ruleset** list, select the ruleset for which this configuration is applicable.

   The Rules and Scoring Management page appears.
8. Expand the rule that you want to delete by clicking the [+] sign.
9. Click **Delete this Rule**.

   You get a message.
10. Click **OK** to complete the task.

    You get the confirmation message.
11. Click **OK**.

    A message stating that the rule is deleted is displayed in the proposed configuration area. In addition, the rule continue to be listed in the **Active** column because it is still active in the production environment.
12. To delete the rule from the production environment, you must migrate your configuration changes to production.

    See "Migrating to Production" (see page 214) for instructions to do so.
13. Refresh all deployed RiskMinder Server instances.

    The rule is deleted.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Uploading Rule List Data

Important! All the configurations and tasks discussed in this section should primarily be performed by Organization Administrators. See "Accessing Organization-Specific RiskMinder Configurations (see page 260)" for more information to access the task page for performing the organization-specific configurations.
If required, these steps can also be performed by Global Administrators. However, they must be performed at the organization level (through the Organizations tab).

If any rule that you deployed requires additional data in the form of a list, then you must perform the tasks in this section. You can add, modify, or delete list data by using the Manage List Data and Category Mappings page in Administration Console. This section describes how to manage data for the following lists:

- Negative Country Lists
- Untrusted IP Lists
- Trusted IP Lists
- Trusted Aggregator Lists
- Data Lists
- Category Mapping Lists

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.

RiskMinder 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, RiskMinder 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

RiskMinder 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 Manage List Data and Category Mappings page to add a country to the Negative Country list or remove a country from the list.

To update the Negative Country list:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **RiskFort Configuration** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.

   The Manage List Data and Category Mappings page is displayed.
8. From the **Select Existing Ruleset** list, select the ruleset that for which this configuration is applicable.
9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Negative Country Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. **Select Negative Countries** that you want to add to the list.

13. Click the > or < button to move selected countries to the desired list.

    You can also click the **>>** or **<<** buttons to move all countries to the desired lists.

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

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

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

    See "Migrating to Production" (see page 214) for instructions to do so.

Configuring Untrusted IP Addresses

The *Untrusted IP address list* is a collection of IP addresses that have been the origin of known anonymizer proxies or fraudulent and malicious transactions in the past. This list is the source of the Negative category discussed in the "Configuring Untrusted IP Types" (see page 192) section.

Use the Manage List Data and Category Mappings page to configure the untrusted IP address ranges for your organization.

Adding or Deleting IP Address Ranges

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

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **RiskFort Configuration** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.

   The Manage List Data and Category Mappings page is displayed.
8. From the **Select Existing Ruleset** list, select the ruleset that for which this configuration is applicable.

   The ruleset configuration information is displayed.
9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Untrusted IP Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. In the **Upload Untrusted IP Ranges** section, select the appropriate mode for writing data:
    - **Append**: This option appends the data that you are uploading to a list or dataset.

      Note: You must select this option if the list does not exist.
    - **Replace**: This option overwrites the existing data in the specified list or dataset.
13. Click **Browse** to navigate to the data file that contains the list of entries.
14. Click **Upload** to complete the task.

15. In the **Add/Delete Untrusted IP Range** section*:*
    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 Untrusted IP Address List.
        - **End IP Address:** If you want to specify a simple range of IP addresses to be added to the Untrusted IP Address List.
    c. Specify the **Information Source** (or vendor) of the untrusted IP address range.
16. Click one of the following buttons, as required:
    - **Add Range:** To add the specified IP address or range to the database.
    - **Delete Range:** To delete the specified IP address or range from the database.

    The appropriate message is displayed.

    The changes are not yet active and are not available to your end users.
17. To make the changes active, you must migrate them to production.

    See "Migrating to Production" (see page 214) for instructions to do so.

Configuring Trusted IP Addresses

In RiskMinder, transactions that either 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, RiskMinder bypasses these transactions from risk evaluations and assigns them a low Score and the ALLOW Advice.

Use the Manage List Data and Category Mappings page to perform the following tasks related to trusted IP addresses and ranges:

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

Adding a Trusted IP Address Range

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

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **RiskFort Configuration** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.

   The Manage List Data and Category Mappings page is displayed.
8. From the **Select Existing Ruleset** list, select the ruleset that for which this configuration is applicable.

   The ruleset configuration information is displayed.
9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Trusted IP Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. Specify the required **IP Address** that will be added to the Trusted IP List.
13. Specify one of the following:
    - **Subnet Mask:** If you want to specify a range of IP addresses based on the subnet mask to be added to the Trusted IP List.

- **End IP Address:** If you want to specify a simple range of IP addresses to be added to the Trusted IP List.

14. Click **Add Range** to add the IP addresses or ranges to the Trusted IP List.

    The Trusted IP List table with the range that you just added appears at the end of the page.

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

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

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

    See "Migrating to Production" (see page 214) for instructions to do so.

Updating a Trusted IP Address Range

To update a trusted IP address or range:

1. Perform the tasks listed from Step 1 through Step 11 in "Adding a Trusted IP Address Range" to display the **Trusted IP List** table.
2. Make the required changes in the **Trusted IP List** table.
3. Select all the affected IP address range(s) in the **Trusted IP List** table.
4. Click **Update** to update the changes that you made.

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

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

   See "Migrating to Production" (see page 214) for instructions to do so.

Deleting a Trusted IP Address Range

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

1. Perform the tasks listed from Step 1 through Step 11in "Adding a Trusted IP Address Range" to display the **Trusted IP List** table.
2. In the **Trusted IP List t**able, select the required IP address range(s) that you want to delete.
3. Click **Delete** to delete the ranges that you selected.
4. To make the changes active, you must migrate them to production.

   See "Migrating to Production" (see page 214) for instructions to do so.

Configuring Trusted Aggregators

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

Transactions originating from (or routed through) aggregators "trusted" to the organization are considered low-risk. For this purpose, RiskMinder provides the ability to configure a list of these aggregators so that all transactions originating from the aggregators' IP addresses are assigned a low Score, and the ALLOW Advice.

RiskMinder uniquely identifies an aggregator by combining their IP address range and a unique Aggregator ID. This Aggregator ID must also be sent to RiskMinder along with the transaction.

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

Use the Manage List Data and Category Mappings page to perform the following tasks related to trusted aggregators:

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

Adding a Trusted Aggregator

To add a trusted aggregator, perform the following tasks:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under **Select Organizations to Modify**, click the link with the organization's name to which you want to apply the rule.
6. Click the **RiskFort Configuration** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link.

   The Manage List Data and Category Mappings page is displayed.

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

   The ruleset configuration information is displayed.

9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Trusted Aggregator Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.
12. Specify the name of the new aggregator in the **Add New Aggregator** field and click **Create.**

    The updated Trusted Aggregator Configuration page appears.

13. Select the **Aggregator** that you want to configure from the drop-down list.
14. Enter the starting IP Address in the **IP Address** field.
15. 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 Aggregator List.
    - **End IP Address:** If you want to specify a simple range of IP addresses to be added to the Trusted Aggregator List.
16. Click **Add Range** to add this IP address or range to the database.

    The Trusted IP List table with the range that you just added for the aggregator appears at the end of the page.

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

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

    See "Migrating to Production" (see page 214) for instructions to do so.

Updating a Trusted Aggregator

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

Important! Periodic rotation or change of the Aggregator IDs is recommended for security purposes. You can decide this rotation duration according to your business rules.

After an ID is updated, you must ensure that the latest Aggregator ID is conveyed to the aggregator. There might be a delay in propagating the Aggregator IDs. In this duration, RiskMinder 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 RiskMinder APIs.

To update an aggregator ID:

1. Complete Step 1 through Step 11 in "Adding a Trusted Aggregator" to display the Trusted Aggregator Configuration information.
2. Select an existing aggregator from the **Aggregator** list.

   The Trusted Aggregator Configuration information with the Aggregator ID(s) for the selected aggregator appears.
3. Click **Update Aggregator ID** to generate a new Aggregator ID.

   The updated Aggregator ID(s) for the aggregator appears, and the next empty Aggregator ID is displayed.
4. In the **Trusted IP List** table, select the aggregator IP addresses or ranges you want to update.
5. Make the required changes and click **Update**.

   The changes are not yet active and are not available to your end users.
6. To make the changes active, you must migrate them to production.

   See "Migrating to Production" (see page 214) for instructions to do so.

Deleting a Trusted Aggregator

To delete a trusted aggregator, perform the following tasks:

1. Complete Step 1 through Step 11 in "Adding a Trusted Aggregator" to display the Trusted Aggregator Configuration information.
2. Select an existing aggregator from the **Aggregator** list.

   The Trusted Aggregator Configuration information appears.
3. In the **Trusted IP List** table, select the aggregator IP addresses or ranges you want to delete.
4. Click **Delete** to delete the selected information.

   The changes are not yet active and are not available to your end users.
5. To make the changes active, you must migrate them to production.

   See "Migrating to Production" (see page 214) for instructions to do so.

Uploading List Data

To upload the data for a rule that uses IN_LIST operator:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Under **Manage Organizations**, click the **Search Organization** link.
4. Click the **Search** button on the Search Organization page to display the list of organizations.
5. Under the **Select Organizations to Modify** section, click the link with the organization's name to which you want to apply the rule.
6. Click the **RiskFort Configuration** tab.
7. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link**.**

   The Manage List Data and Category Mappings page appears.
8. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.
9. Select the **Manage List Data** option.
10. From the **Select List Type** list, select **Other Lists**.
11. From the **Select List** drop-down list, select the list identifier that you specified while creating the corresponding list.

    The updated page appears.
12. In the **Upload File Or Enter Data** section, select the appropriate mode for writing data:
    - **Append**: This option appends the data that you are uploading to a list or dataset.

      Note: You must select this option if the list does not exist.
    - **Replace**: This option overwrites the existing data in the specified list or dataset.
13. Do *one* of the following:
    - Click **Browse** to navigate to the data file that contains the list of entries (separated by a newline character.)

      or
    - Type in the entries in the **Enter Data** field, if a data file does not exist.

      Important! Ensure that the entries are separated by a newline character (ENTER).
14. Click **Upload** to complete the task.

Uploading Category Mappings Data

To upload the data for a rule that uses IN_CATEGORY operator:

1. Ensure that you are logged in as a GA.
2. Activate the **Organizations** tab.
3. Click the **Search** button on the page to display the list of organizations.
4. Under the **Select Organizations to Modify** section, click the link with the organization's name to which you want to apply the rule.
5. Click the **RiskFort Configuration** tab.
6. Under the **Rules Management** section on the side-bar menu, click the **Manage List Data and Category Mappings** link**.**

   The Manage List Data and Category Mappings page appears.
7. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.

   The configuration information for the specified ruleset appears.
8. Select the **Manage Category Mappings** option.
9. From the **Select Category Mapping** list, select the mapping set identifier that you specified while creating the corresponding list.

   The updated page appears.
10. In the **Upload File Or Enter Classification Data** section, select the appropriate mode for writing data:
    - **Append**: This option appends the data that you are uploading to a list or dataset.

      Note: You must select this option if the list does not exist.
    - **Replace**: This option overwrites the existing data in the specified list or dataset.
11. Perform *one* of the following:
    - Click **Browse** to navigate to the data file that contains the list of entries (separated by a newline character.)

      or
    - Type in the entries in the **Enter Data** field, if a data file does not exist.

      Important! Ensure that the entries are separated by a newline character (ENTER).
12. Click **Upload** to complete the task.

Migrating to Production

RiskMinder is shipped with **default** settings for the following rules and configurations:

- Trusted IP Address and Aggregators
- Untrusted IP Address
- Negative Country List
- Exception User
- Unknown User
- Device MFP Not Match
- User Velocity
- Unknown DeviceID
- User Not Associated with DeviceID
- Device Velocity
- Zone Hopping
- Miscellaneous Rule Configurations
- Scoring

In addition, you can also configure:

- New rules
- Callouts

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

When all data is configured according to your requirements, then the Proposed data can be converted to *Active data* (the **Active** column on respective configuration page) by migrating it to production and refreshing the RiskMinder Server cache. See "arrfclient: Server Refresh and Shutdown Tool" (see page 299) tool for more information.

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

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

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

To migrate changes from Proposed configuration area to the Active data area:

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

   The Migrate to Production page appears.
4. On the page, either:
   - Select the **Select All Rulesets** option, if you want to migrate all the changes that you made to all the configured rulesets.

     or
   - Select a specific ruleset from the **Select Ruleset(s)** list to migrate the changes that you made to this ruleset.
5. Click **Migrate**.

   The page to confirm the action is displayed.
6. On the confirmation page, click **Confirm** to start the *migration process*.

   Note: Based on the volume of data that you are migrating to production, the migration process might take a few minutes.

   After the migration is completed, the "The proposed data has been successfully migrated to Production." message is displayed.
7. Refresh the RiskMinder Server cache. See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Chapter 9: Configuring Callouts

Important! All the configurations and tasks discussed in this section can be performed by **Global Administrators** to apply the rules globally or **by Organization Administrators** to apply the rules for an organization.

See "Managing Organization-Specific RiskMinder Configurations" (see page 259) for more information to access the task page for performing the organization-specific configurations:

A *Callout* is a custom component (which can be written in a programming language of your choice) to modify or augment the standard functionality of RiskMinder. A Callout, typically, is an external process. As a result, it resides "outside" the RiskMinder Server context and is hosted on a separate HTTPS-based server. Being an external process, you must configure a Callout by using the Administration Console, so that it is invoked when required.

This section describes the types of Callouts that RiskMinder supports and how to configure these Callouts to meet your business requirements. In addition, this section also walks you through the deployment, configuration, and use of the Sample Callout that is shipped in the RiskMinder package:

- Understanding Callouts (see page 218)
- Configuring Callouts (see page 222)
- Working with the Sample Callout (see page 227)

Note: Ensure that the administrator performing configuration-related activities has the required privileges to perform these operations. For more information on the privileges available to administrators at each level, see "Summary of Administrative Privileges" (see page 59).

After you configure a Callout, the changes are not immediately **active** (available to your end users.) You *must* use the **Migrate to Production** link in the side-bar menu of Administration Console to "move" all **proposed** configuration changes to your production database. See "Migrating to Production" (see page 214) for steps to migrate to production.

Understanding Callouts

Based on your business requirements, you can write your own custom Evaluation logic and Scoring logic, which if implemented, will run at your application-end, independent of RiskMinder Server. 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: RiskMinder is shipped with a basic Sample Callouts WAR file (riskfort-3.1.01-sample-callouts.war) that demonstrates how you can write and implement simple Evaluation and Scoring Callouts. See "Working with the Sample Callout" (see page 227) 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 RiskMinder's Negative Country, Untrusted 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 a Callout is deployed, you *must* enable it by using the Callout Configuration page for it to take effect.

Callout Implementation

Note: Implementation of Callouts is optional.

If you have implemented a Callout, then RiskMinder Server reads all configurations related to the Callout from the database and caches the information on startup. During a transaction:

1. RiskMinder Server calls the Callout framework *after* executing all pre-defined and new rules (in case of Evaluation Callout) or the standard Scoring Engine (in case of Scoring Callout.)

   Note: The Callout framework is a part of RiskMinder Server and just like any other RiskMinder 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 RiskMinder Server and prepares the HTTP or HTTPS data.

   Note: RiskMinder supports both one-way and two-way SSL-based connections between RiskMinder 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 the 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 RiskMinder Server.

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

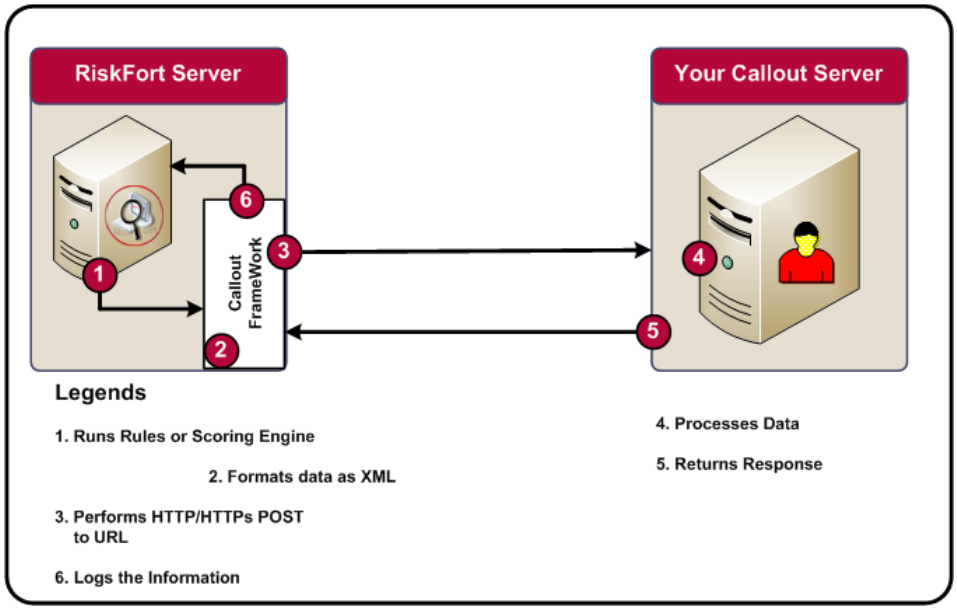
   Note: The time-out period can be configured by using Administration Console.

4. Your Callout processes the data by using custom logic.

5. Your Callout then returns an appropriate response to the Callout framework, which forwards the same to RiskMinder Server.

6. RiskMinder Server logs all the information returned by the framework for reporting and auditing purposes.

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



Note: If you are implementing an Evaluation as well as a Scoring Callout, then you can either implement them on the same server or on separate servers.

Types of Callouts

RiskMinder supports the following types of Callouts:

- Evaluation Callout (see page 221)
- Scoring Callout (see page 222)

Evaluation Callout

An Evaluation Callout is executed as part of risk evaluation. If an Evaluation Callout is implemented, then:

1. RiskMinder executes all Standalone and Combination rules and invokes the Callout framework.
2. The RiskMinder Callout framework formats the data in XML format.
3. The RiskMinder 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 RiskMinder Evaluation rule.
   - **Rule results** for each Evaluation rule that was executed.
   - **Additional Inputs**, if any, that are provided by the RiskMinder SDK to RiskMinder Server as input data.
4. Your Callout uses the data passed by RiskMinder to process its custom logic.
5. Your Callout then returns the following information to RiskMinder:
   - **Rule result** in the form of Y (SUCCESS) or N (FAILURE).
   - **Modifier string** with additional information, if any, to be used by the Scoring Callout (if implemented.)

   Note: RiskMinder Server does not process the modifier string at all. If a Scoring Callout also has been implemented, then RiskMinder Server POSTs this data to the Scoring Callout.
   - **Annotation string** that contains the reason or the description sent back to RiskMinder Server.

   Note: This information is used for logging (in the database), reporting, and auditing purposes.
6. RiskMinder Server logs the information returned by your Callout.

Scoring Callout

A *Scoring Callout* is executed *after* the standard RiskMinder Scoring logic has executed. If a Scoring Callout is implemented, then:

1. RiskMinder Server executes the standard Scoring program and invokes the Callout framework.
2. The RiskMinder Callout framework formats the data in XML format.
3. The RiskMinder Callout framework performs an HTTP or HTTPS POST of the following information to your Scoring Callout:
   - **Overall Score** computed by the standard RiskMinder built-in Scoring Engine.
   - **Rule results** for each Evaluation rule that was executed.
   - **Additional Inputs**, if any, that are provided by the calling application as part of the evaluateRisk() API call.
   - **Modifier string** originally returned by the Evaluation Callout.
4. Your Callout uses the data passed by RiskMinder to process its custom logic.
5. Your Callout then returns the following information to RiskMinder:
   - **Final Score** in the form of an integer in the range [0 – 100].

   Note: The score returned by the Scoring Callout always overrides the Score computed by the RiskMinder Scoring Engine. If you want to retain the score computed by RiskMinder'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 RiskMinder 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), reporting, and auditing purposes.
6. RiskMinder Server logs the information returned by your Callout.

Configuring Callouts

Use the Callout Configuration page for:

- Configuring Evaluation Callout (see page 223)
- Configuring Scoring Callout (see page 225)

Note: RiskMinder is shipped with a basic Sample Callouts WAR file (riskfort-3.1.01-sample-callouts.war) that demonstrates how you can write and implement Evaluation and Scoring Callouts. See Working with the Sample Callout (see page 227) for more information on deploying and configuring this file.

Configuring Evaluation Callout

To configure an Evaluation Callout, perform the following steps:

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

   The Callout Configuration page appears.
4. Ensure that the **Evaluation Callout** option is selected and click **Next**.

   The Evaluation Callout Configuration page appears.
5. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.

   The updated Evaluation Callout Configuration page is displayed.
6. In the table, under the **Proposed** column:
   a. Select the appropriate SSL option for **Server Authentication SSL**.

      Important! If you want to configure SSL-based communication between RiskMinder 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 RiskMinder 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 RiskMinder Server and your Callout, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is set to **YES**.
      - If you do not want to configure any SSL-based connection, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is also set to **NO**.

   c. Specify the URL at which the Callout is available against **Callout URL**.

      - If **Server Authentication SSL** is set to **YES** *or* **Client Authentication SSL** is set to **YES**, then the URL of Evaluation Callout *must* begin with *https://*.
      - If both **Server Authentication SSL** is set to **NO** *and* **Client Authentication SSL** is set to **NO**, then the URL of Evaluation Callout *must* begin with *http://*.

   d. Specify the value of **Connection Timeout** in milliseconds.

      Connection Timeout indicates the time in which connection between RiskMinder Server and your Callout will expire.

   e. Specify the value of **Read Timeout** in milliseconds.

Read Timeout indicates the time in which RiskMinder 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**.

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

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

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

   See "Migrating to Production" (see page 214) for instructions to do so.

9. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Configuring Scoring Callout

To configure a Scoring Callout, perform the following steps:

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

   The Callout Configuration page appears.
4. Select the **Scoring Callout** option and click **Next**.

   The Scoring Callout Configuration page appears.
5. From the **Select Existing Ruleset** list, select the ruleset for which this configuration is applicable.

   The updated Scoring Callout Configuration page is displayed.
6. In the table, under the **Proposed** column:
   a. Select the appropriate SSL option for **Server Authentication SSL**.

      Important! If you want to configure SSL-based communication between RiskMinder 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 RiskMinder 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 RiskMinder Server and your Callout, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is also set to **YES**.
      - If you do not want to configure any SSL-based connection, then you must select **NO**. In this case, you must ensure that the **Server Authentication SSL** is also set to **NO**.

   c. Specify the URL at which the Callout is available against **Callout URL**.

      - If **Server Authentication SSL** is set to **YES** *or* **Client Authentication SSL** is set to **YES**, then the URL of Evaluation Callout *must* begin with *https://*.
      - If both **Server Authentication SSL** is set to **NO** *and* **Client Authentication SSL** is set to **NO**, then the URL of Evaluation Callout *must* begin with *http://*.

   d. Specify the value of **Connection Timeout** in milliseconds.

      Connection Timeout indicates the time in which connection between RiskMinder Server and your Callout will expire.

   e. Specify the value of **Read Timeout** in milliseconds.

Read Timeout indicates the time in which RiskMinder 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 SS**L 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**.

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

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

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

   See "Migrating to Production" (see page 214) for instructions to do so.

9. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Working with the Sample Callout

RiskMinder 3.1.01 is shipped with a basic and non-GUI Sample Callouts WAR file (riskfort-3.1.01-sample-callouts.war) that demonstrates:

- The basic operations (invocation and post-processing) of RiskMinder Server from your custom program.
- The integration of your Callout with RiskMinder.

This Sample Callouts WAR file is automatically installed as a part of **Complete** installation of RiskMinder. As a part of **Custom** installation, you *must* select the **RiskFort Server** component to access this WAR file.

Important! Sample Callouts *must* be deployed on the same application server where RiskMinder Server is installed.

This section covers:

- Deploying Sample Callouts (see page 228)
- Configuring RiskMinder Server to Communicate With Sample Callouts (see page 229)

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 RiskMinder on your application server:

1. Navigate to Settings > Control Panel > Administrative Tools > Services.
2. Stop the application server services.
3. Deploy the riskfort-3.1.01-sample-callouts.war file from the following location: `<install_location>\Arcot Systems\samples\java\`

   Note: Although you will also see riskfort-3.1.01-sample-callouts.war in the package, it is recommended that you deploy the Sample Application WAR file from the preceding location.
4. Navigate to Settings > Control Panel > Administrative Tools > Services.
5. Restart the application server services.

On UNIX-Based Platforms

To deploy the Sample Callouts shipped with RiskMinder on your application server:

1. Stop the application server services.
2. Deploy the riskfort-3.1.01-sample-callout.war file from the following location: `<install_location>/arcot/samples/java/`
3. Restart the application server services.

Configuring RiskMinder Server to Communicate With Sample Callouts

Note: The XSD for the request and response XML is available in the <*install_location*>\Arcot Systems\docs\riskfort\Arcot-Riskfort-3.1.01-CallOutInterface-xsds.zip file.

To configure the Sample Callouts, perform the following steps:

1. Perform the tasks listed from Step 1 through Step 5 in "Configuring Evaluation Callout" (see page 223) to display the **Evaluation Callout Configuration** page.
2. Under the **Proposed** column of the table:
   a. Select **NO** for **Server Authentication SSL**.
   b. Select **NO** for **Client Authentication SSL**

      Note: The client here is the Sample Callout.
   c. Specify the following against the **Callout URL** option:

      http://<host>:CA Portal/riskfort-3.1.01-sample-callouts/SampleEvalCalloutServlet

      Here, *<host>* refers to the host name or IP address of the server where your Callouts WAR is deployed and *CA Portal* refers to the port on which this server is available.
   d. Specify the value of **Connection Timeout** in milliseconds. The default value is 30000 milliseconds.
   e. Specify the value of **Read Timeout** in milliseconds. The default value is 30000 milliseconds.
   f. Specify useful details about the Callout against **Callout Description**.
   g. Click **Save** to save the changes that you just made.
3. Perform the tasks listed from Step 1 through Step 5 in "Configuring Scoring Callout" (see page 225) to display the **Scoring Callout Configuration** table.
4. Under the **Proposed** column of the table:
   a. Select **NO** for **Server Authentication SSL**.
   b. Select NO for Client Authentication SSL.

      Note: The client here is the Sample Callout.
   c. Specify the following against the **Callout URL** option:

      http://<host>:CA Portal/riskfort-3.1.01-sample-callouts/SampleScoringCalloutServlet

      Here, *<host>* refers to the host name or IP address of the server where your Callouts WAR is deployed and *CA Portal* refers to the port on which this server is available.

d. Specify the value of **Connection Timeout** in milliseconds. The default value is 30000 milliseconds.

e. Specify the value of **Read Timeout** in milliseconds. The default value is 30000 milliseconds.

f. Specify useful details about the Callout against **Callout Description**.

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

All the changes that you made until now are not yet active, and not available to your end users.

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

See "Migrating to Production" (see page 214) for instructions to do so.

Chapter 10: Managing Organizations

Note: Most of the tasks in this section can be performed by a Global Administrator (GA) or an Organization Administrator (OA) if they have the required scope to the organization.

In the Administration Console, an *organization* can either map to a complete enterprise (or a company) or a specific division, department, or other entities within the enterprise. The organization structure provided by Administration Console is flat. In other words, organizational hierarchy (in the form of parent and child organizations) is *not* supported, and all organizations are created at the same level as the Default Organization. For more information on Default Organization, see "Setting the Default Organization" (see page 44).

The larger the enterprise, the more complex its organization structure. As a result, management of organizations is a critical part of administration. The organization management operations supported by RiskMinder include:

- Creating and Activating Organizations (see page 232)
- Searching for Organizations (see page 243)
- Updating Organization Information (see page 244)
- Uploading Users and User Accounts in Bulk (see page 248)
- Viewing the Status of the Bulk Data Upload Request (see page 252)
- Refreshing Organization Cache (see page 253)
- Deactivating Organizations (see page 254)
- Activating Organizations (see page 255)
- Activating Organizations in Initial State (see page 256)
- Deleting Organizations (see page 257)

Note: In addition to the preceding list of tasks related to organization management, OAs can also manage organization-specific configurations. For more information, see "Managing Organization-Specific RiskMinder Configurations" (see page 259).

Creating and Activating Organizations

You can create an organization either in the RiskMinder repository or in your existing LDAP-based directory server implementations, such as Microsoft Active Directory, SunOne Directory Server, or CA Directory Server.

Note: In case of a small deployment, you can rename the Default Organization, instead of creating a new organization.

Based on your implementation, this section guides you through the procedure used for:

- Creating Organizations in RiskMinder Repository (see page 232)
- Creating Organizations in LDAP Repository (see page 236)

Privileges Required

To create and activate an organization, you must ensure that you have the appropriate privileges to do so. Only MA and GAs can create and activate all organizations.

Creating Organizations in RiskMinder Repository

To create an organization in the RiskMinder repository:

1. Ensure that you are logged in with the required privileges to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Create Organization** link to display the Create Organization page.
4. Enter the details of the organization, as discussed in the following table.

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. **Note:** You have to specify this value to log in to this organization, *not* the Display Name of the organization.
Display Name	Enter a unique descriptive name for the organization. **Note:** This name appears on all other Administration Console pages and reports.
Description	Provide a description for the administrators who will manage this organization. **Note:** You can provide additional details for later reference for the organization by using this field.

Field	Description
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators who belong to this organization. Administration Console supports the following types of authentication mechanisms: ■ **Basic User Password** This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators can log in to the Console by specifying their user ID and password. ■ **LDAP User Password** This mechanism is applicable only for LDAP organizations. The authentication policy is defined in the LDAP directory service. If you select this option, then administrators must use the credentials stored in LDAP to log in to the Console. **WebFort User Password** This is the AuthMinder user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by the AuthMinder Server. To use this mechanism, you must have CA AuthMinder installed and configured. For more information, see the *CA AuthMinder Installation and Deployment Guide*.
Key Label Configuration RiskMinder enables you to use hardware- or software-based encryption of your sensitive data. You can choose the encryption mode by using the arcotcommon.ini configuration file. For more information, see the topic titled "HSM Encryption Settings" in the *CA RiskMinder Installation and Deployment Guide*. Irrespective of hardware or software encryption, AuthMinder and RiskMinder use Global Key Label for encrypting user and organization data. If you are using hardware encryption, then this label serves only as a reference (or pointer) to the actual 3DES key stored in the HSM device. In this case, the key label that you specify must match the HSM key label. However, in the case of software-based encryption, this label acts as the key.	
Use Global Key	This option is selected by default. Deselect this option if you want to override the Global Key Label you specified in the bootstrap process and specify a new key label that will be used for encrypting organization-specific data.

Field	Description
Key Label	If you deselected the **Use Global Key** option, then specify the new key label that you want to use for the organization.
Storage Type	This option indicates whether the encryption key is stored in the database (**Software**) or the HSM (**Hardware**).
Localization Configuration	
Use Global Configuration	Select this option to use the localization parameters that are configured at the global level.
Date Time Format	If you deselected the **Use Global Configuration** option, then specify the Date Time format that you want to use for this organization.
Preferred Locale	If you deselected the **Use Global Configuration** option, then select a preferred locale for this organization.
User Data Location	
Repository Type	Select **Arcot Database**. By specifying this option, the user and administrator details for the new organization will be stored in the RDBMS repository supported by RiskMinder.
Custom Attributes Use this section to provide additional information specific to the organization you are creating.	
Name	Name of the custom attribute.
Value	Value of the custom attribute.

1. Click **Next.**
2. The Select Attribute(s) for Encryption page appears.
3. In the **Attribute(s) for Encryption** section, do one of the following:
   a. Select **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration.

      or

   b. Select the attributes that you want to encrypt from the **Available Attributes for Encryption** list and move them to the **Attributes Selected for Encryption** list.

      Click the > or < buttons to move selected attributes to the desired list. You can also click the >> or << buttons to move all attributes to the desired lists.
4. Click **Next**.

   The Add Administrators page appears.

   Note: This page is *not* displayed, if all the administrators currently present in the system have the scope to manage all organizations.
5. From the **Available Administrators** list, select the administrators who will manage the organization and click the **>** button to add the administrator to the **Managing Administrators** list.

   The **Available Administrators** list displays all the administrators who can manage the new organization.

   Note: If some administrators have scope to manage all organizations in the system, then you will not see the corresponding entries for those administrators in this list.

   The **Managing Administrators** list displays the administrators that you have selected to manage this organization.
6. Click **Next** to proceed.

   The Configure Account Type page appears.

   Note: That:
   – This page is not displayed if you have not created any account types.
   – Global account types will be selected by default.
7. In the **Assign Account Types** section, select account types from the **Available** list and click the > button to move them to the **Selected** list.
8. Click **Next** to proceed.

   The Configure Account Custom Attributes page appears.

   Note: This page is not displayed if you did not select any account types on the previous page.
9. Provide **Custom Attributes** for your **Account Type**, and click **Next**.

   The Configure Email/Telephone Type page appears.

10. Specify the mandatory and optional email address and telephone numbers the user must provide.
11. Click **Skip** to use the email and telephone types configured at the system level and move to the next page, or click **Save** to save your changes.

    The Activate Organization page appears.
12. Click **Enable** to activate the new organization.
    A message box appears.
13. Click **OK** to complete the process.

    Note: If you do not choose to activate the organization, the organization is created in Initial state. You can activate the organization later. For instructions to do so, see "Activating Organizations in Initial State" (see page 256).
14. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

    Caution: If you have configured the attribute encryption set, account types, and email and telephone types while creating the organization, ensure that you refresh *both* the system configuration and the organization cache. If you do not refresh the organization-level cache, the system gets into an unrecoverable state.

Creating Organizations in LDAP Repository

To support LDAP user directories, you must create an organization in the LDAP repository and then map the RiskMinder database attributes with the LDAP attributes. To do so:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Create Organization** link to display the Create Organization page.
4. Enter the details of the organization, as discussed in the following table.

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. **Note:** You can use Administration Console to log in to this organization, by specifying this value, *not* the Display Name of the organization.

Field	Description
Display Name	Enter a unique descriptive name for the organization. **Note:** This name appears on all other Administration Console pages and reports.
Description	Provide a description for the administrators who will manage this organization. **Note:** You can provide additional details for later reference for the organization by using this field.
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators who belong to this organization. Administration Console supports the following two types of authentication mechanisms: ■ **Basic User Password** This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators can log in to the Console by specifying their ID and plain text password. ■ **LDAP User Password** This mechanism is applicable only for LDAP organizations. The authentication policy is defined in the LDAP directory service. If you select this option, then administrators must use the credentials stored in LDAP to log in to the Console. ■ **WebFort User Password** This is the AuthMinder user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by AuthMinder Server. To use this mechanism, you must have AuthMinder installed and configured. For information about deploying AuthMinder, see the *CA AuthMinder Installation and Deployment Guide*.
Key Label Configuration	
Use Global Key	This option is selected by default. Deselect this option if you want to override the Global Key Label you specified in the bootstrap process and specify a new key label to encrypt organization-specific data.
Key Label	If you deselected the **Use Global Key** option, then specify the new key label that you want to use for the organization.
Storage Type	This option indicates whether the encryption key is stored in the database (**Software**) or the HSM (**Hardware**).
Localization Configuration	

Field	Description
Use Global Configuration	Select this option to use the localization parameters that are configured at the global level.
Date Time Format	If you deselected the **Use Global Configuration** option, then specify the Date Time format that you want to use for this organization.
Preferred Locale	If you deselected the **Use Global Configuration** option, then select a preferred locale for this organization.
User Data Location	
Repository Type	Select **Enterprise LDAP**. By specifying this option, the user details for the new organization will be stored in the LDAP repository that you will specify on the next page.
Custom Attributes	
Name	Name of the custom attribute.
Value	Value of the custom attribute.

1. Click **Next.**

   The Create Organization page to collect the LDAP repository details appears.

2. Enter the details, described in the following table, to connect to the LDAP repository.

Field	Description
Host Name	Enter the host name of the system where the LDAP repository is available.
Port Number	Enter the port number on which the LDAP repository service is listening.
Schema Name	Specify the LDAP schema used by the LDAP repository. This schema specifies the types of objects that an LDAP repository can contain, and specifies the mandatory and optional attributes of each object type. Typically, the schema name for Active Directory is user and for SunOne Directory and CA Directory Server, it is inetorgperson.

Field	Description
Base Distinguished Name	Enter the base Distinguished Name of the LDAP repository. This value indicates the starting node in the LDAP hierarchy to search in the LDAP repository. For example, to search or retrieve a user with a DN of cn=rob laurie, ou=sunnyvale, o=arcot, c=us, you must specify the base DN as the following: ou=sunnyvale, o=arcot, c=us **Note:** Typically, this field is case sensitive and searches all subnodes under the provided base DN.
Redirect Schema Name	Specify the name of the schema that provides the definition of the "*member*" attribute. You can search for users in the LDAP repository by using the Base DN defined for an organization. But this search returns only the users who belong to a specific Organization Unit (OU). An LDAP administrator might want to create a group of users who belong to different Organization Units for controlling access to an entire group, and might want to search for users from different groups. When the administrator creates groups, user node DNs are stored in a "member" attribute within the group node. By default, UDS does not allow search and DN resolution based on attribute values. Redirection enables you to search for users who belong to different groups within LDAP, based on specific attribute values for a particular node. Typically, the redirect schema names are as follows: ■ Active Directory: group ■ SunOne Directory: groupofuniquenames ■ CA Directory Server: groupOfUniqueNames
Connection Type	Select the type of connection that you want to use between Administration Console and the LDAP repository. Supported types are: ■ TCP ■ One-way SSL ■ Two-way SSL
Login Name	Enter the complete distinguished name of the LDAP repository user who has the privilege to log in to repository sever and manage the Base Distinguished Name. For example, uid=gt,dc=arcot,dc=com
Login Password	Enter the password of the user provided in the Login Name.

Field	Description
Server Trusted Root Certificate	Enter the path for the trusted root certificate who issued the SSL certificate to the **LDAP** server by using the **Browse** button, if **One-way SSL** or **Two-way SSL**: option is selected.
Client Key Store Path	Enter the path for the key store that contains the client certificate and the corresponding key by using the **Browse** button, if the **Two-way SSL** option is selected. **Note:** You must upload either PKCS#12 or JKS key store type.
Client Key Store Password	Enter the password for the client key store, if the **Two-way SSL** option is selected.

1. Click **Next** to proceed.

   The page to map the repository attributes appears.

2. On this page:

   a. Select an attribute from the **Arcot Database Attributes** list, then select the appropriate attribute from the **Enterprise LDAP Attributes** list that needs to be mapped with the RiskMinder database attribute, and click **Map**.

      Important! Mapping of the UserName attribute is compulsory. Ensure that you map the UserName attribute to an LDAP attribute that uniquely identifies the user. If you are using Active Directory, then map *UserName* to sAMAccountName. If you are using SunOne Directory Server, then map *UserName* to uid. If you are using CA Directory Server, then map *UserName* to cn.

      For Active Directory, you must map STATUS to userAccountControl.

   b. Repeat the process to map multiple attributes, until you finish mapping all the required attributes.

      Note: You do not need to map all the attributes in the **Arcot Database Attributes** list. You only need to map the attributes that you will use.

      The attributes that you have mapped will be moved to the **Mapped Attributes** list.

      If required, you can unmap the attributes. If you want to unmap a single attribute at a time, then select the attribute and click **Unmap**. However, if you want to clear the **Mapped Attribute** list, then click **Reset** to unmap all the mapped attributes. You cannot unmap the UserName attribute after you have activated the organization.

   c. If you specified the **Redirect Schema Name** in the previous page, you must select the search attribute from the **Redirect Search Attribute** list.

      Typically, the attributes are as follows:

      - Active Directory: member
      - SunOne Directory: uniquemember
      - CA Directory Server: uniqueMember

3. Click **Next** to proceed.

   The Select Attribute(s) for Encryption page appears.

4. In the **Attribute(s) for Encryption** section, do one of the following:

   a. Select **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration.

      or

   b. Select the attributes that you want to encrypt from the **Attributes Available for encryption** list and move them to the **Attributes Selected for encryption** list.

Click the > or < buttons to move selected attributes to the desired list. You can also click the >> or << buttons to move all attributes to the desired lists.

5. Click **Next**.

   The Add Administrators page appears.

   Note: This page is *not* displayed, if all the administrators currently present in the system have the scope to manage all organizations.

6. From the **Available Administrators** list, select the administrators who will manage the organization and click the **>** button to add the administrator to the **Managing Administrators** list.

   Note: Assigning organization to administrators can be done at any time by updating the scope of existing administrators or by creating new administrators to manage the organization.

   The **Available Administrators** list displays all the administrators who can manage the new organization.

   Note: If some administrators have the scope to manage all organizations in the system, then you will not see the corresponding entries for those administrators in this list.

   The **Managing Administrators** list displays the administrators that you have selected to manage this organization.

7. Click **Next** to proceed.

   The Configure Account Type page appears.

   Note: This page is not displayed if you have not created any account types.

8. In the **Assign Account Types** section, select account types from the **Available** list and click the > button to move them to the **Selected** list.

9. Click **Next** to proceed.

   The Configure Account Custom Attributes page appears.

   Note: This page is not displayed if you did not select any account types on the previous page.

10. Provide **Custom Attributes** for your **Account Type**, and click **Next**.

    The Activate Organization page appears.

    Note: The UserName mapping *cannot* be changed or updated after the organization is activated.

11. Click **Enable** to activate the new organization.

    A warning message appears.

12. Click **OK** to complete the process.

13. Refresh *all* deployed RiskMinder Server instances.

    See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Caution: If you have configured the attribute encryption set, account types, and email and telephone types while creating the organization, ensure that you refresh *both* the system configuration and the organization cache. If you do not refresh the organization-level cache, the system gets into an unrecoverable state.

Searching for Organizations

As long as you do not need to update, activate, or deactivate an organization, you do not need privileges to search. However, you *must* have the scope over the organizations that you are searching. For example, an OA can search for a target organization *if* that organization is in their purview.

Searching Organizations

You can search for organizations by their display name and status. To search for one or more organizations:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the partial or complete information of the required organization. You can select the following options to broaden your search:

   Note: In the **Organization** field, you must enter the partial or complete display name of the organization and *not* the actual organization name.

   - **Initial** (to display the organizations that have been created but have not been activated yet.)
   - **Active** (to display the organizations that have been created and have been activated.)
   - **Inactive** (to display the organizations that have been disabled.)
   - **Deleted** (to display the organizations that have been deleted.)
5. Click **Search** to display the page with all the matches for the specified criteria.

Updating Organization Information

By using Administration Console, you can update the following information for an organization:

- **Organization information** that includes organization display name, description, and status, the administrators that manage the organization, account types assigned to the organization, email/telephone types configured, and attribute encryption set ("Updating the Basic Organization Information" (see page 245))
- **RiskMinder-specific configurations** for the organization that include credential profiles, authentication policies, extensible configurations, and the assigned default configurations ("Updating RiskMinder-Specific Configurations" (see page 247))

Privileges Required

To update an organization, you must ensure that you have the appropriate privileges and scope. The MA can update all organizations. GAs and OAs can update the information for all organizations in their scope.

Updating the Basic Organization Information

To update the basic organization information:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page appears.
6. In the **Organization Details** section, edit the required fields (**Display Name** and **Description**).
7. Edit the **Administrator Authentication Mechanism**, if required.

   You can edit the authentication mechanism only if there no administrators exist for this organization.
8. In the **Localization Configuration** section, you can:

   a. Choose to **Use Global Configuration**.

   or

   b. Edit the **Date Time Format** and **Preferred Locale**.
9. In the **Custom Attributes** section, edit the **Name** and **Value** fields, if required.
10. Click **Next** to proceed with additional configurations:

    - If the organization was created in the **Arcot Repository**, then do the following:

    1. On the Select Attribute(s) for Encryption page, **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration, or select the attributes that you want to encrypt from the **Available Attributes for Encryption** list to the **Attributes Selected for Encryption** list, and click **Next**.

       You cannot update attributes if users have already been created in the organization.

    2. On the Update Administrators page, update the administrators who will manage the organization, and click **Next**.

    3. On the Configure Account Type page, configure the account types by moving them from the **Available** list to the **Selected** list and click **Next**.

       You cannot deselect global account types.

4. On the Configure Account Custom Attributes page, add custom attributes for the accounts and click **Next**.
5. On the Configure Email/Telephone Type page, configure the mandatory and optional Email address and Telephone Type for the users, and click **Save** to complete the process.

- If the organization was created **in the LDAP repository**, then Edit Organization page appears. To update the organization details:

a. Use the information in Creating Organizations in LDAP Repository (see page 236) to update the fields, as required, and click **Next** to display the page to edit the Repository Attribute Mappings.

b. Except for the UserName mapping, you can edit the other mappings. Click **Next** to display the Select Attribute(s) for Encryption page.

c. On the Select Attribute(s) for Encryption page, **Use Global Configuration** if you want to use the global settings for your attribute encryption set configuration, or select the attributes that you want to encrypt from the **Available Attributes for Encryption** list to the **Attributes Selected for encryption** list, and click **Next**.

d. You cannot update the attributes if users have already been created in the organization. In the case of LDAP, even a simple search operation for users in the LDAP repository registers the users in the database. So, you cannot update the attributes if you have searched for users in the LDAP repository.

e. On the Update Administrators page, update the administrators who will manage the organization and click **Next.**

f. On the Configure Account Type page, configure the account types by moving them from the **Available** list to the **Selected** list and click **Update** to save your changes and complete the process.

You cannot deselect global account types.

11. Refresh *all* deployed RiskMinder Server instances.

See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Updating RiskMinder-Specific Configurations

To update the RiskMinder configurations of an organization:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button to display a list of organizations matching the search criteria.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization to display the Organization Information page appears.
6. Activate the **RiskFort Configuration** tab to display the links for RiskMinder configurations in the task panel.

   See "Managing Organization-Specific RiskMinder Configurations" (see page 259) for detailed information on these configurations.

Uploading Users and User Accounts in Bulk

RiskMinder now allows you to upload users and user accounts in bulk through Administration Console. You need a comma-separated value (CSV) input file to upload information for multiple users and user accounts.

Uploading Users in Bulk

The first line in the CSV input file to upload users must be as follows:
`#UserID,fName,mName,lName,status,pam,pamURL,EmailAddr,telephoneNumber,INFOLIST#`

Caution: The preceding first (template) line is *always* required. If you do not specify this line, then the bulk user upload operation will fail.

Note the following when you create the csv input file to upload users:

- The csv file should have one header starting and ending with #. All the other field names should be provided between these # symbols.
- Only the UserID entry is mandatory. The other entries are optional.
- If the user you are trying to upload already exists, the user details are updated.
- You can provide up to five email addresses and five telephone numbers. In this case, you must specify the header, as follows:
  `#UserID,fName,mName,lName,status,pam,pamURL,EmailAddr,EMAIL.2,EMAIL.3,EMAIL.4,EMAIL.5,telephoneNumber,PHONE.2,PHONE.3,PHONE.4,PHONE.5,INFOLIST#`

The entries in the file are described in the following table.

Entry	Description
UserID	The unique ID of the user.
fName	The first name of the user.
mName	The middle name of the user.
lName	The last name of the user.
status	The status of the user. Possible values are: ■ INITIAL ■ ACTIVE
pam	The personal authentication message
pamURL	The URL where the user's personal authentication message image is available
EmailAddr	The contact email ID of the user.

Entry	Description
telephoneNumber	The complete phone number of the user with the international code. For example, US phone numbers should start with 1.
INFOLIST	Additional information about the user. Values must be separated by semi-colons. For example: age=25;favsport=cricket

A sample file, for example, can contain:

```
#UserID,fName,lName,status,EmailAddr,telephoneNumber,PHONE.2,INFOLIST#
mparker,martin,parker,ACTIVE,mparker@ca.com,12345,9999,age=29;favsport=cricket
jhume,john,hume,ACTIVE,jhume@ca.com,3939292,203939393,age=32;favbook=fiction
fantony,francis,antony,ACTIVE,fantony@ca.com,130203,29888,age=25;favfood=pizza#
```

Uploading User Accounts in Bulk

The first line in the CSV input file to upload user accounts must be as follows:

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountID
Attribute2,accountIDAttribute3,customAttr1,customAttr2,customAttr3
,customAttr4,customAttr5,customAttr6,customAttr7,customAttr8,custo
mAttr9,customAttr10#
```

Caution: The preceding first (template) line is *always* required. If you do not specify this line, then the bulk user account upload operation will fail.

Note the following when you create the csv input file to upload user accounts:

- Only the UserID, accountType, and accountID entries are mandatory. The other entries are optional.
- You must have created the user in the system.
- You must have created the account type and assigned it to the organization.
- You must have created custom attributes for the account type.
- You can provide up to 10 custom attributes for an account type.

The entries in the file are described in the following table.

Entry	Description
UserID	The unique ID of the user.
accountType	The account type associated with the accountID.
accountID	The alternate ID of the user.

Entry	Description
status	The status of the account ID. Possible values are: ■ [0-9]: INITIAL ■ [10-19]: ACTIVE ■ [20-29]: INACTIVE
accountIDAttribute1	Attribute of the accountID. You can provide up to a maximum of three account ID attributes.
customAttr1	Custom attribute for the user account.

A sample file, for example, can contain:

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,acco
untIDAttribute3,customAttr1,customAttr2#
prush,ONLINE_BANKING,OB_ID1,10,login,password,image,chicago,music
jhume,SAVINGS,SA_ID1,10,interest,deposit,check,florida,soccer
```

To create multiple users and user accounts in the RiskMinder database:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select the organization to which you want to upload users and user accounts in bulk.
6. Under the **Basic Organization Information** section, click the **Bulk Upload** link to display the Bulk Data Upload page.
7. In the **Bulk Upload** section:
   a. Select **Upload User Accounts** or **Upload Users** from the **Bulk Upload Operation** drop-down list.
   b. Click **Browse** to navigate to the required csv file that contains the user account or user entries.
   c. Provide a **Description** for the operation.
8. Click **Upload** to upload user accounts or users in bulk.
9. After the operation completes, you will see a Request ID in the message.
10. (**IMPORTANT**) Carefully note the Request ID.

    You will need it to view the status of the bulk data upload operation.

Viewing the Status of the Bulk Data Upload Request

To view the status of the bulk data upload request:

1. Ensure that you are logged in with the required privileges and scope to perform this operation.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select the organization for which you want to view the status of the bulk upload request.
6. Under the **Basic Organization Information** section, click the **View Bulk Requests** link to display the Search Bulk Requests page.
7. In the Search Bulk Requests page:
   a. Enter the Request ID that you noted down earlier in Step 10 in "Uploading Users and User Accounts in Bulk" (see page 248).

      or

   b. Select a **Status** based on which you want to view the bulk request.

      or

   c. Select an **Operation**, depending on whether you want to view **Upload Users** or **Upload User Accounts** requests.
8. Click **Search** to display the table.
9. In case of failure, click the **Request ID** link to get more information on the bulk request.
10. Click the **No. of failed operations** link to view the reason why the operation failed.

In the case of failed operations for a request, the **Export Failures** button is enabled. Click **Export Failures** to export all the failed operations to a csv file. You can then correct the errors in the exported file, and resubmit the file for bulk upload.

Refreshing Organization Cache

Organization configurations that do not refer to the global configuration, such as attribute encryption set, localization configuration, and email and telephone types are cached at the organization level. When you make changes to these configurations at the organization level, you must refresh the organization cache for the changes to take effect.

Note: The MA can refresh the cache of all organizations. The GA and OA can refresh the cache of all organizations within their scope.

To refresh the organization cache:

1. Ensure that you are logged in with the required privileges and scope to refresh the organization cache.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select the organizations whose cache you want to refresh.
6. Click **Refresh Cache**.
7. Click **OK** in the dialog box to confirm your cache refresh request.

   A message with a Request ID for the current cache refresh request is displayed. You can check the status of your cache refresh request by clicking the **Check Cache Refresh Status** link and selecting this **Request ID**.

Note: Refreshing the cache of one organization does not affect the response time of transactions going on at that time for other organizations.

Deactivating Organizations

When you want to prevent all administrators of an organization from logging in to Administration Console and end users of the organization from authenticating to your application by using RiskMinder mechanisms, you deactivate the organization.

Privileges Required

To deactivate an organization, you must ensure that you have the appropriate privileges and scope. The MA can deactivate all organizations. GAs and OAs can deactivate all organizations in their scope.

Deactivating Organizations

To deactivate one or more organizations:

1. Ensure that you are logged in with the required privileges and scope to deactivate the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select one or more organizations that you want to deactivate.
6. Click **Deactivate** to disable the selected organizations.

   A message box appears.
7. Click **OK** to confirm the deactivation.
8. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Activating Organizations

You might need to activate a deactivated organization. In this case, you must select the **Inactive** option while specifying the search criteria on the Search Organization page.

Privileges Required

To activate an organization, you must ensure that you have the appropriate privileges and scope. The MA can activate all organizations. GAs and OAs can activate all organizations in their scope.

Activating Organizations

To activate a deactivated organization:

1. Ensure that you are logged in with the required privileges and scope to activate the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select one or more organizations that you want to activate again.
6. Click **Activate** to activate the selected organizations.

   A message appears.
7. Click **OK** to confirm the activation.
8. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Activating Organizations in Initial State

Sometimes you might start creating an organization, but not activate it. For example, you might specify the **Organization Information** and **User Data Location** on the Create Organization page, but not specify the details of the LDAP repository or the administrators who will manage the organization. In such cases, the organization is created, but is not active and is not typically visible in searches (unless you search by selecting the **Initial** option).

Such organizations remain in the Initial state in the system, unless you activate them. Later, if you try to create a new organization with the same details as an organization in Initial state, the system does not allow you to, because the organization exists.

Privileges Required

To activate an organization in Initial state, you must ensure that you have the appropriate privileges and scope. MA can activate all organizations. GAs and OAs can activate all organizations in their scope.

Activating Organizations in Initial State

To activate an organization that is in the **Initial** state:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the partial or complete information of the required organization and select the **Initial** option.
5. Click **Search** to display the page, with all the matches for the specified criteria.
6. Select the organizations that you want to activate.
7. Click **Activate** to enable the selected organizations. A message appears.
8. Click **OK** to confirm the activation.
9. Refresh *all* deployed RiskMinder Server instances.

   See "Refreshing the Cache" (see page 37) for instructions on how to do this.

Deleting Organizations

After an organization is deleted, the administrators associated with the organization can no longer log in to it by using Administration Console and the end users who belong to this organization cannot authenticate. However, the information related to the organization is still maintained in the system. The administrator who has scope on the deleted organization can read the organization details.

Privileges Required

To delete an organization, you must ensure that you have the appropriate privileges and scope. The MA can delete all organizations. GAs and OAs can delete all organizations in their scope.

Deleting Organizations

To delete an organization:

1. Ensure that you are logged in with the required privileges and scope to delete the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select one or more organizations that you want to delete, and click **Delete**.

   A message appears.
6. Click **OK** to confirm the deletion.

Chapter 11: Managing Organization-Specific RiskMinder Configurations

Note: To manage the configurations of an organization, you (**Organization Administrator**) must ensure that you have the appropriate privileges and scope.

A **Master Administrator** *cannot* manage any organization-specific configurations. GAs and OAs can manage the configurations for all organizations in their scope.

Although you can create a copy of the "templatized" rule settings configured by the Global Administrators (GAs) (as discussed in Managing Global Configurations (see page 147)), you might want to override them to meet the specific business requirements of the organizations in your purview.

When you set rule configurations at the level of an organization, the changes are restricted to the specific organization where they were set. Also, the changes you make to the configurations are *not* applied automatically. You need to refresh all server instances to apply these configuration changes.

As an OA, if you have the scope on the given organizations, then you can perform the following tasks:

- Accessing Organization-Specific RiskMinder Configurations (see page 260)
- Creating Rulesets (see page 261)
- Assigning Rulesets (see page 262)
- Using Global Rule Configurations (see page 263)
- Configuring RiskMinder for An Organization (see page 263)

Accessing Organization-Specific RiskMinder Configurations

The organization-specific configurations are similar to the global configurations, but navigation paths to their task page is different. To access the task page for performing the organization-specific configurations:

1. Ensure that you are logged in with the required privileges and scope to update the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page appears.
6. Activate the **RiskFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane.
7. Configure the required rulesets and risk evaluation rules.

   Note: See "Managing Global Configurations" (see page 147) for detailed information on how to configure the required rules and assign them, as needed. The operations discussed in "Managing Global Configurations" **(see page 147)** are for the global level, but the configurations discussed here are for the organization level. The configurations for both are the same; only the approach to access the task page is different, as explained at the beginning of this section.

Creating Rulesets

As discussed in "Understanding Rulesets" (see page 157), a ruleset is a collection of rules configured by a Global Administrator (GA) or an Organization Administrator (OA.)

Important! If created by a GA, a ruleset is *only available for copying for individual organizations*. Therefore, an OA must either create a new ruleset by copying the global ruleset, or must re-create the ruleset again at the organization level.

See "Creating Rulesets" (see page 158) for detailed information on how to create a ruleset.

Important! After you create a ruleset, you *must* migrate it to production for it to be available for activation.

Assigning Rulesets

After an OA creates a ruleset for their organization and migrates it to production, you must activate this ruleset for an organization within your scope for it to take effect. To assign an existing ruleset to the current organization:

1. Ensure that you are logged in with the required privileges and scope to assign rulesets.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page appears.
6. Activate the **RiskFort Configuration** tab.
7. Under the **Ruleset** section, click the **Assign Ruleset** link.

   The Assign Ruleset page appears.
8. Select the ruleset that you want to activate from the **Select Ruleset to assign** list.
9. Click **Save** to make the specified ruleset active for the current organization.

Deleting Rulesets

This release of RiskMinder allows you to delete rulesets that are not currently assigned to an organization. To delete a ruleset:

1. Ensure that you are logged in with the required privileges and scope to delete rulesets.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page appears.
6. Activate the **RiskFort Configuration** tab.
7. Under the **Ruleset** section, click the **Delete Ruleset** link.

   The Delete Ruleset page appears.
8. **Select the Ruleset** that you want to delete.
9. Click **Delete**.
10. Click **OK** in the confirmation message box to complete the task.

    The ruleset is deleted.

Using Global Rule Configurations

Although you can change the rule configurations individually for every organization in your scope, most of your organizations might be using the same configuration settings repeatedly. Also, setting rule configurations for individual organizations can be a cumbersome task if a large number of organizations are configured. In this case, you might want to tweak the global configurations set by a GA for the rules so that you do not need to specify the same setting every time.

When a GA, who has scope to your organizations, sets rule configurations at the global level, all your organizations inherit these settings. You can use these settings *by creating a copy*.

Use the **Advanced Option** section that you see on the Create Ruleset page. The section is collapsed, and you will need to click on the **+** sign to expand the section and see the available option.

You have the option to copy the configuration from an existing Ruleset.

Select the **Copy from an Existing Ruleset** option, and then select the name of the ruleset whose configuration you want to copy from the drop-down list.

Configuring RiskMinder for an Organization

In addition to creating and assigning rulesets, as an Organization Administrator (OA), you can perform most of the tasks mentioned in "Managing Global Configurations" (see page 147). These include:

- Configuring the out-of-the-box rules for the organizations in your scope.

  See "Configuring Out-of-the-Box Rules" (see page 162) for detailed steps.
- Deploying new rules for the organizations in your scope.

  See "Adding New Rules" (see page 163) for detailed steps.
- Configuring Callouts for the organizations in your scope.

  See "Configuring Callouts" (see page 217) for detailed steps.
- Migrating configurations to production for the organizations in your scope.

  See "Migrating to Production" (see page 214) for detailed steps.

Chapter 12: Managing Administrators

The types of administrators and their roles and responsibilities depend on the size of your deployment. A small, single-organization deployment can have just one Master Administrator (MA) and a Global Administrator (GA) who administers the organization for end users. On the other hand, a very large multi-organization deployment can find it necessary to have multiple GAs who, based on the complexity of the deployment and the number of end users, can further delegate their organization and user management duties among several Organization Administrators (OAs) and User Administrators (UAs).

See "Supported Roles" (see page 16) for information on supported administrative roles. This section covers the following administrator management operations:

- Creating Administrators (see page 266)
- Changing Profile Information for Administrators (see page 268)
- Searching Administrators (see page 269)
- Updating Administrator Information (see page 270)
- Changing Administrator Role to User (see page 271)
- Configuring Account IDs for Administrators (see page 272)
- Deactivating Administrators (see page 275)
- Deactivating Administrators Temporarily (see page 276)
- Activating Administrators (see page 277)
- Deleting Administrators (see page 278)

Note: In addition to the operations discussed in this section, the Master Administrator has the privilege to create "Custom Roles" (see page 23) that are derived from the existing default roles supported by RiskMinder.

Creating Administrators

An administrator can create other administrators who belong to the same level or to the lower levels in the administrative hierarchy *and* have the same or lesser scope. For example:

- The MA can create all other types of administrators.
- GAs can create the following *within* their scope:
  - Other GAs
  - OAs
  - UAs
- OAs can create the following *within* their scope:
  - Other OAs
  - UAs

To create an administrator in an organization that is configured for Basic Username-Password credential:

1. Ensure that you are logged in with the required privileges and scope to create the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Create Administrator** link to display the Create Administrator page.
4. In the **Administrator Details** section, enter the details of the administrator. The following table explains the fields on this page.

Input	**Description**
User Name	The unique user name for the administrator.
Organization	The display name of the organization to which the administrator belongs. **Note:** This is *not* the organization that this administrator will manage.
First Name	The first name of the administrator.
Middle Name (optional)	The middle name, if any, of the administrator.
Last Name	The last name of the administrator.

5. In the **Email Address(es)** section, enter the email address of the administrator for the email types configured for the organization.
6. In the **Telephone Number(s)** section, enter the phone number to contact the administrator.

   If multiple telephone types are configured, you *must* enter values for all the mandatory telephone types.
7. In the **Custom Attributes** section, enter the **Name** and **Value** of any attributes you want to add, such as office location.
8. Click **Next** to proceed.

   The next page appears.
9. On this page:
   - Specify the role of the new administrator from the **Role** drop-down list.
   - In the **Set Password** section, set and confirm the password for the administrator.
   - In the **Manages** section, select the organizations that the administrator will have scope on, and perform one of the following:
     - Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.

       or
     - Select the required organizations from the **Available Organizations** list and click the **>** button to add these organization to the **Selected Organizations** list.

     The **Available Organizations** list displays *all* the organizations that are available in the scope of the administrator creating this new account. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.
10. Click **Create** to save the changes, create the account, and activate it.
11. Communicate the new password to the administrator.

Changing Profile Information for Administrators

The profile information for an account includes:

- Personal information (first, middle, and last names and contact information).
- Password for the account.
- Administrator preferences, such as Preferred Organization (the organization that will be selected by default in the **Organization** fields for all administrator-related tasks that you might perform in future), date time format, locale, and timezone information.

Note: An administrator can change their account's profile information at any time. To change the information for any other administrative account, see "Updating Administrator Information" (see page 270).

To change the administrator profile information for your account, if it was created with basic Username-Password credential:

1. Ensure that you are logged in t*o your account.*
2. In the **Header** frame, click the <ADMINISTRATORNAME> link to display the My Profile page.
3. Edit the required settings in the sections on this page:
   a. Edit the fields in the **Personal Information** section, as needed.
   b. If you want to change the current password, then in the **Change Password** section, enter the **Current Password,** and specify a new password in the **New Password** and **Confirm Password** fields.
   c. In the **Administrator Preferences** section:
      - Select the **Enable Preferred Organization** option, and select an organization from the **Preferred Organization** list. This organization will be selected for all administrator-related tasks that you perform from now on.
      - Specify the preferred **Date Time Format**.
      - Select the preferred **Locale** for your instance of Administration Console.
      - Select the required option from the **Time Zone** list.
4. Click **Save** to change the profile information.

Searching Administrators

Note: As long as you do not need to update, activate, or deactivate an administrative account, you do not need privileges to search. However, you *must* have the scope over the organizations that the administrator belongs to. For example, a UA can search for administrators in the target organization *if* that organization is in their purview.

To search for administrators with the specified criteria:

1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Specify the search criteria to display the list of administrators. You can:
   - Search for administrators by specifying the partial or complete information of the administrator in the fields on this page.
   - Search for administrators by specifying the organization's Display Name.
   - Search for administrators by not specifying any criteria and just clicking **Search**.
   - Click the **Advanced Search** link to display the Advanced Search page to search for the required administrators by specifying their Status or Role.

   Note: In the **User Status** section, you can search for **Current Users** based on the user status (Active, Inactive, or Initial) or you can search for **Deleted Users**.
5. Select **Enable search by Accounts** if you want to search for administrators based on account IDs also.
6. Specify the required details of the administrators and click **Search**.

   A list of administrators matching the search criteria appears.

Updating Administrator Information

Note: To update administrator information, you must ensure that you have the appropriate privileges and scope. The MA can update any administrator. The GAs can update all the administrators (including other GAs) in their scope, *except* the MA account. The OAs can update all other OAs and UAs in their purview, while UAs can only update their peers within their scope.

To update an administrator's basic details (such as first, middle, and last names, contact information) and their administrative role, password, and management scope:

1. Ensure that you are logged in with the required privileges to update the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the corresponding page.
4. Enter the partial or complete information of the administrator whose account you want to update (as discussed in the preceding section) and click **Search**.

   A list of administrators matching the search criteria appears.
5. Click the <*user name*> link of the administrator whose account you want to edit.

   The Basic User Information page appears.

   Note: This page also displays the **User Account Information** (**Account Type**, **AccountID**, and **Status**) if any account type was configured.
6. Click **Edit** to change the administrator information on this page.
7. In the **User Details** section, edit the required fields (**First Name**, **Middle Name**, and **Last Name**).
8. In the **Email Address(es)** section, edit the email addresses for the email types configured for the organization.
9. In the **Telephone Number(s)** section, edit the telephone numbers for the telephone types configured for the organization.
10. In the **Custom Attributes** section, edit the **Name** and **Value** of the custom attributes.
11. You can either click **Save** to save the changes made and return to the User Information page, *or* you can click **Next** to proceed with additional configurations.

    Note: If you don't see a **Next** button, it means that no account type has been configured for the organization. In this case, click **Update Administrator Details** and go to Step 14.

    If you click **Next**, then the User Account page appears.
12. In the **User Account** section:
    - Edit the **Account Type** and **Status** fields.

- Expand **Advanced Attributes** to add **AccountID Attributes** for the account ID.

Note: If this is the first account ID you are creating, you must click **Add** to add an account ID before you can update it. For more information on adding an account ID, see "Creating Account IDs" (see page 273).

- Provide values for any **Custom Attributes** that are configured for the account type.

13. Click **Update Administrator Details**.

    The **Update Administrator** page appears.

14. In the **Role** section on this page, change the role of the administrator by using the **Role** drop-down list.
15. In the **Set Password** section:
    - Set the **Password** and **Confirm Password** for the administrator.
    - Select **Lock** to lock the administrator's credentials for the **Credential Lock Period**, which you can specify in the **From** and **To** fields.
16. In the **Manages** section, select the organizations that the administrator will manage.

    You can also remove the organization from the administrator's scope by moving the specific organization from **Selected Organizations** to **Available Organizations**.
17. Click **Save** to save the updates.

Changing Administrator Role to User

You can change the role of an administrator to an user. For example, an administrator in the IT department might have moved to the Engineering department. In this case, we would want to retain the user details, but remove the administrative privileges for the user.

To change the role of an administrator to user:

1. Perform Step 1 to Step 13, as described in the preceding section, "Updating Administrator Information" (see page 270).

   The Update Administrator page appears.
2. On the Update Administrator page, click **Change Role to User**.
3. Click **OK** in the confirmation dialog box that appears.
4. You get the following message:

   Successfully demoted the administrator to user.

Configuring Account IDs for Administrators

An account ID is an alternate ID to identify the user, in addition to the user name. After you have configured the account types that your organization will use, you can associate one account ID per user for any of these account types. For more information on account types, see "Configuring the Account Type" (see page 45).

Note: To configure an account ID for an account type, you must ensure that you have the appropriate privileges and scope to update the user account. The MA can update any user account. The GAs can update all user accounts in their scope. The OAs and UAs can update the user accounts in their purview.

Creating Account IDs

To create an account ID:

1. Ensure that you are logged in with the required privileges and scope to update the administrator information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator whose account you want to update (as discussed in the preceding section) and click **Search**.

   A list of administrators matching the search criteria appears.
5. Click the <*user name*> link of the administrator whose account you want to edit.

   The Basic User Information page appears.
6. Click **Edit** to open the Update Administrator page.
7. Click **Next** to display the User Account page.
8. Select the **Account Type** for which you want to add the account ID.
9. Specify the unique **AccountID** in the text box.

   This combination of account type and account ID will be used to identify the user in addition to the user name.
10. Select the **Status** of the user account from the drop-down list.
11. If required, expand the **Advanced Attributes** section, and do the following:
    - Provide attributes for the account ID you are creating.

    Note: You can specify up to a maximum of three account ID attributes for any account ID.
    - Provide values for any **Custom Attributes** that are configured for the account type.
12. Click **Add** to add the account ID.

Updating Account IDs

Note: You cannot change the account ID once it is created. You can only change the status of the user account and add or delete account ID attributes and custom attributes.

To update an account ID:

1. Complete Step 1 through Step 7 in "Creating Account IDs" (see page 273) to display the User Account page.
2. Select the **Account Type** for which you want to update the account ID information.
3. If required, change the **Status** of the user account from the drop-down list.
4. If required, expand the **Advanced Attributes** section, and provide attributes for the account ID you are creating and custom attributes, if any.
5. Click **Update** to save your changes.

Deleting Account IDs

To delete an account ID:

1. Complete Step 1 through Step 7 in "Creating Account IDs" (see page 273) to display the User Account page.
2. Select the **Account Type** for which you want to delete the account ID.
3. Click **Delete** to delete the account ID.

Deactivating Administrators

To prevent an administrator from logging in to their account for security reasons, you can deactivate them instead of deleting them. If you deactivate an administrator, the administrator is locked out of their account, and cannot log in unless the account is re-activated again.

Note: To deactivate an administrator, you must ensure that you have the appropriate privileges and scope. The MA can deactivate any administrator, while GAs can deactivate all administrators (including other GAs) in their scope, *except* the MA account. The OAs can deactivate all other OAs and the UAs in their purview, while UAs can only deactivate their peers within their scope.

To deactivate an administrator:

1. Ensure that you are logged in with the required privileges to deactivate the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator whose account you want to deactivate and click **Search**.

   You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive) or their roles (GA, OA, or UA).

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators you want to deactivate.
6. Click **Deactivate** to deactivate the selected administrator.

Deactivating Administrators Temporarily

Temporarily deactivating the administrator differs from *deactivating* the administrator (see "Deactivating Administrators" (see page 275)). When you temporarily deactivate the administrator, the administrator is automatically activated when the end of the lock period is reached. But when you deactivate an administrator, you must manually activate them again whenever you want to provide access to them.

To temporarily deactivate an administrator, you must specify the **Start Lock Date** and **End Lock Date** for the period that you want the administrator to be locked. When the **End Lock Date** is reached, the administrator is automatically activated.

To temporarily deactivate an administrator:

1. Ensure that you are logged in with the required privileges to deactivate the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator whose account you want to deactivate and click **Search**.

   You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive) or their roles (GA, OA, or UA).

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators you want to deactivate temporarily.
6. Click **Deactivate Temporarily**.

   The Deactivate User Temporarily dialog box appears.
7. In the **Starting From** section, select the start lock **Date** and the **Time**.
8. In the **To** section, select the end lock **Date** and the **Time**.
9. Click **Save** to save your changes.

   Note: If you do not specify any value for the **Starting From** fields, the account is locked from the current time. If you do not specify an end lock **Date**, the account is locked forever.

Activating Administrators

You might need to activate a deactivated administrator. For example, you might deactivate an administrator if the administrator is on long vacation. This helps prevent unauthorized access to that administrator information.

You cannot search directly for the deactivated administrators by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You *must* perform an **Advanced Search** for such administrators and use the **Inactive** option in the **Current Users** section to search.

Note: To activate an administrator, you must ensure that you have the appropriate privileges and scope. The MA can activate any administrator, while the GAs can activate all administrators (including other GAs) in their scope, *except* the MA. The OAs can activate all other OAs and UAs in their purview, while the UAs can only activate their peers within their scope.

To activate a deactivated administrator:

1. Ensure that you are logged in with the required privileges to activate the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive).

   The Advanced Search page appears.
5. Enter the partial or complete information of the administrator in the **User Details** section.
6. In the **User Status** section, for **Current Users**, select the **Inactive** and **Initial** options to search for all inactive or initial administrators.
7. Click **Search** to display the list of all administrators matching the search criteria.
8. Select the administrators you want to activate.
9. Click **Activate** to activate the administrator.

Deleting Administrators

Administrator information in RiskMinder includes personal information (first name, middle name, last name, email address, and telephone number), credentials, and accounts. When you delete an administrator from Administration Console, the credential and account information must also be deleted along with the personal information. RiskMinder supports the cascaded user deletion feature by which all credential, account, and risk-related information for an administrator is also deleted when the administrator is deleted.

If you create a new administrator with the same name as a previously deleted administrator, then the new administrator *does not* automatically assume the privileges of the previously deleted administrator. If you need to duplicate a deleted administrator, then you must manually re-create all privileges.

Note: To delete an administrator, you must ensure that you have the appropriate privileges and scope. The MA can delete any administrator, while the GAs can delete all administrators (including other GAs) in their scope, *except* the MA account. The OAs can delete all other OAs and UAs in their purview.

However, the UAs *cannot* delete their peers within their scope.

To delete an administrator:

1. Ensure that you are logged in with the required privileges to delete the administrator.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator you want to delete and click **Search**.

   You can also click the **Advanced Search** link to search for **Current Users** based on their status (active, inactive, or initial) or their roles (GA, OA, or UA).

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators you want to delete.
6. Click **Delete**.

   Note: Even though you have deleted the administrator, their account information is still maintained in the database.

Chapter 13: Managing Users

RiskMinder works with your application to manage strong authentication for administrators and end users. RiskMinder allows you to create users directly through Administration Console. Managing user information is a critical part of maintaining a secure system. The end user management operations supported by RiskMinder for this purpose include:

- Creating Users (see page 279)
- Searching Users (see page 281)
- Updating User Information (see page 282)
- Promoting Users to Administrators (see page 284)
- Configuring Account IDs for Users (see page 285)
- Deactivating Users (see page 288)
- Deactivating Users Temporarily (see page 289)
- Activating Users (see page 290)
- Deleting Users (see page 291)

Creating Users

Every end user of your online application system is referred to as a user in Administration Console. Global Administrators (GAs), Organization Administrators (OAs), and User Administrators (UAs) can create users for organizations within their scope.

To create a user:

1. Ensure that you are logged in with the required privileges and scope to create the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Create User** link to display the Create User page.
4. In the **User Details** section, enter the details of the user. The following table explains the fields on this page.

Field	Description
User Name	The unique user name.
Organization	The display name of the organization to which the user belongs.

Field	Description
First Name (optional)	The first name of the user.
Middle Name (optional)	The middle name, if any, of the user.
Last Name (optional)	The last name of the user.

5. In the **Email Address(es)** section, enter the email address of the user.
6. In the **Telephone Number(s)** section, enter the phone number to contact the user.
7. Select whether you want the user to be in the **Initial** state or you want to make the user **Active**.
8. In the **Custom Attributes** section, enter the **Name** and **Value** of any attributes you want to add, such as office location.
9. Click **Create User** to create the user.

Searching Users

Note: As long as you do not need to create, update, activate, or deactivate a user, you do not need privileges to search. However, you *must* have the scope over the organization that the target user belongs to. For example, a GA from one organization can search for users in another organization, *if* that organization is in their purview.

To search for users with the specified criteria:

1. Ensure that you are logged in with the appropriate scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Specify the search criteria to display the list of users. You can:
   - Search for users by specifying the partial or complete information of the user in the fields on this page.

     Note: Specifying partial information in the fields works only if the fields are *not* marked for encryption. If any of the fields on this page have been marked for encryption, then you *must* specify the complete value for the search to function properly.
   - Search for users by specifying the organization's Display Name.
   - Search for users by not specifying any criteria and just clicking **Search**.
   - Click the **Advanced Search** link to display the Advanced Search page to search for users by specifying their Status or Role.
5. Specify the required details of the users and click **Search**.

   A list of users matching the search criteria appears.

Updating User Information

Note: To update a user's account settings, you must ensure that you have the appropriate privileges and scope. The MA can update information of any user. The GAs can update all users in their scope. The OAs and UAs can update information for users in their purview.

To update a user's basic details (such as first, middle, and last names, contact information):

1. Ensure that you are logged in with the required privileges and scope to update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user whose account you want to update (as discussed in the preceding section) and click **Search**.

   A list of administrators matching the search criteria appears.
5. Click the <*user name*> link of the user whose account you want to edit.

   The Basic User Information page appears.

   Note: The Basic User Information page also displays the **User Account Information** (**Account Type**, **AccountID**, and **Status**) if any account type was configured.
6. Click **Edit** to change the user information on this page.
7. In the **User Details** section, edit the required fields (**First Name**, **Middle Name**, **Last Name**).
8. In the **Email Address(es)** section, edit the email addresses for the email types configured for the organization**.**
9. In the **Telephone Number(s)** section, edit the telephone numbers for the telephone types configured for the organization.
10. Update the **User Status**, if required.
11. Edit the **Name** and **Value** of **Custom Attributes,** if required.
12. You can either click **Save** to save the changes made and return to the User Information page, *or* you can click **Next** to proceed with additional configurations.

    Note: The **Next** button is available only if you have configured accounts for the organization.

    If you click **Next**, then the User Account page appears.
13. In the **User Account** section:
    - Edit the **Status**, if required.

- Expand **Advanced Attributes** to add **AccountID Attributes** and **Custom Attributes** for the account ID.

Note: If this is the first account ID you are creating, you must click **Add** to add an account ID before you can update it. For more information on adding an account ID, see "Creating Account IDs" (see page 286).

14. Click **Update** to save your changes.

Promoting Users to Administrators

Note: To promote a user to an administrator, you must ensure that you have the appropriate privileges and scope. The MA can promote any user. The GAs can promote users to OA, UA, or GA for organizations within their administrative purview. The OAs can promote users to OA or UA for organizations within their administrative purview. The *UAs can*not promote users to administrators.

To update a user's administrative role, password, and management scope:

1. Ensure that you are logged in with the required privileges and scope to create administrators and update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user whose account you want to update (as discussed in the preceding section) and click **Search**.

   A list of users matching the search criteria appears.
5. Click the <*user name*> link of the user whose account you want to edit.

   The Basic User Information page appears.
6. Click **Edit** to open the Update User page.
7. If the user's **First Name**, **Last Name**, **Email address(es), Telephone Number(s)** are not specified, enter the same. These attributes are mandatory for administrators.
8. Click **Next** to display the User Account page.

   Note: If no account type is configured for the user's organization, then the **Change Role to Administrator** button is displayed in the Update User page itself.
9. On the User Account page, click **Change Role to Administrator** to display the Create Administrator page.
10. On this page:
    - Specify the role of the new administrator from the **Role** drop-down list.
    - Enter the password for the administrator in the **Password** and **Confirm Password** fields.
    - In the **Manages** section, select the organizations that the administrator will have scope on, and perform the following:
      - Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.

        or
      - Select the required organizations from the **Available Organizations** list and click the **>** button to add these organization to the **Selected Organizations** list.

The **Available Organizations** list displays *all* the organizations that are available in the scope of the logged in administrator. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.

11. Click **Create** to save the changes and create and activate the administrator.

Configuring Account IDs for Users

An account ID is an alternate ID to identify the user, in addition to the user name. After you have configured the account types that your organization will use, you can associate one account ID per user for any of these account types. For more information on account types, see "Configuring the Account Type" (see page 45).

Note: To configure an account ID for an account type, you must ensure that you have the appropriate privileges and scope to update the user. The MA can update any user. The GAs can update all users in their scope. The OAs and UAs can update the users in their purview.

Creating Account IDs

To create an account ID:

1. Ensure that you are logged in with the required privileges and scope to update the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user for whom you want to create the account ID, and click **Search**.

   You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive) or their roles (GA, OA, or UA).

   The Search Results page appears, with all the matches for the specified criteria.
5. Click the <*user name*> link of the user whose account you want to edit.

   The Basic User Information page appears.

   Note: This page also displays the **User Account Information** (**Account Type**, **AccountID**, and **Status**) for the account types configured.
6. Click **Edit** to open the Update User page.
7. Click **Next** to display the User Account page.
8. Select the **Account Type** for which you want to add the account ID.
9. Specify the unique **AccountID** in the text box.

   This combination of account type and account ID will be used to identify the user in addition to the user name. You must ensure that the account type and account ID combination is unique for a particular organization.
10. Select the **Status** of the user account from the drop-down list.
11. If required, expand the **Advanced Attributes** section, and do the following:

    a. Provide **AccountID Attributes** for the account ID.

    Note: You can specify up to a maximum of three attributes for any account ID.

    b. Provide values for any **Custom Attributes** that are configured for the account type.
12. Click **Add** to add the account ID.

Updating Account IDs

Note: You cannot change the account ID once it is created. You can only change the status of the user account and add account ID attributes.

To update an account ID:

1. Complete Step 1 through Step 7 in "Creating Account IDs" (see page 286) to display the User Account page.
2. Select the **Account Type** for which you want to update the account ID.
3. If required, change the **Status** of the user account from the drop-down list.
4. If required, expand the **Advanced Attributes** section, and provide **AccountID Attributes** and **Custom Attributes** for the account ID you are updating.
5. Click **Update** to save your changes.

Deleting Account IDs

To delete an account ID:

1. Complete Step 1 through Step 7 in "Creating Account IDs" (see page 286) to display the User Account page.
2. Select the **Account Type** for which you want to delete the account ID.
3. Click **Delete** to delete the account ID.

Deactivating Users

To prevent a user from logging in to their account for security reasons, you can deactivate them instead of deleting them. If you deactivate users, then they are locked out of their account, and cannot log in unless they are activated again.

Note: To deactivate a user, you must ensure that you have the appropriate privileges and scope. The MA can deactivate any user, while the GAs can deactivate all users (including other GAs) within their scope. The OAs and UAs can deactivate all users in their purview.

To deactivate a user:

1. Ensure that you are logged in with the required privileges and scope to deactivate the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user whose account you want to disable and click **Search**.

   You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive).

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users to deactivate.
6. Click **Deactivate** to deactivate the selected user.

Deactivating Users Temporarily

Temporarily deactivating the user differs from *deactivating* the user (see "Deactivating Users" (see page 288)). When you temporarily deactivate the user, the user is automatically activated when the end of the lock period is reached. But when you deactivate a user, you must manually activate them again whenever you want to provide access to the user.

To temporarily deactivate a user, you specify the **Start Lock Date** and **End Lock Date** for which the user is locked. When the **End Lock Date** is reached, the user is automatically activated.

To temporarily deactivate a user:

1. Ensure that you are logged in with the required privileges and scope to deactivate the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user to deactivate and click **Search**.

   You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive).

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users to deactivate temporarily.
6. Click **Deactivate Temporarily**.
7. The Deactivate User Temporarily page appears.
8. In the **Starting From** section, select the start lock **Date** and **Time**.
9. In the **To** section, select the end lock **Date** and **Time**.
10. Click **Save** to save your changes.

    Note: If you do not specify any value for the **Starting From** fields, the user is locked from the current time. If you do not specify an end lock **Date**, the user is locked forever.

Activating Users

You might need to activate a deactivated user. For example, you might deactivate an administrator if the administrator is on long vacation. This helps to prevent unauthorized access to that administrator's information.

You cannot search directly for deactivated users by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You must perform an **Advanced Search** for such users and use the **Inactive** option in the **Current Users** section to search.

Note: To activate a user, you must ensure that you have the appropriate privileges and scope. The MA can activate any user, while the GAs can activate all users within their scope. The OAs and UAs can activate all users in their purview.

To activate a locked-out user:

1. Ensure that you are logged in with the required privileges to activate the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive).

   The Advanced Search page appears.
5. Enter the partial or complete information of the user in **User Details** section.
6. In the **User Status** section, for **Current Users**, select the **Inactive** and **Initial** options to search for all inactive or initial users.
7. Click **Search** to display the list of all users matching the search criteria.
8. Select the users you want to activate.
9. Click **Activate** to activate the user.

Deleting Users

User information in RiskMinder includes personal information (first name, middle name, last name, email address, and telephone number), credentials, and accounts. When you delete a user from Administration Console, the credential and account information must also be deleted along with the personal information. RiskMinder supports the cascaded user deletion feature by which all credential, account, and risk-related information for a user is also deleted when the user is deleted.

If you create a new user with the same name as a previously deleted user, then the new user *does not* automatically assume the privileges of the previously deleted user. If you need to duplicate a deleted user, then you must manually re-create all privileges.

Note: To delete a user, you must ensure that you have the appropriate privileges and scope. The MA can delete any user, while the GAs can delete all users (including other GAs), *except* the MA account, within their scope. The OAs and UAs can delete all users in their purview.

To delete a user:

1. Ensure that you are logged in with the required privileges to delete the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user you want to delete and click **Search**.

   You can also click the **Advanced Search** link to search for users based on their status (active, inactive, or initial) or their roles (User).

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users you want to delete.
6. Click **Delete**.

   Note: After you delete a user, the user information is deleted from the database. However, the user history is archived for billing purposes.

Chapter 14: Tools for System Administrators

This section discusses the tools provided by RiskMinder that administrators can use to monitor and manage the system. The following table lists the tools and their location.

Tool	Location
DBUtil	**On Windows:** <*install_location*>\Arcot Systems\tools\win **On UNIX Platforms:** <*install_location*>/arcot/tools/<*platform_name*>
arrfversion arrfclient arrfserver arrfupload	**On Windows:** <*install_location*>\Arcot Systems\bin\ **On UNIX Platforms:** <*install_location*>/arcot/bin/

This section describes the following tools:

- DBUtil: RiskMinder Database Tool (see page 294)
- arrfversion: RiskMinder Modules Version Display Tool (see page 299)
- arrfclient: Server Refresh and Shutdown Tool (see page 299)
- arrfserver: RiskMinder Server Tool (see page 302)
- arrfupload: Quova Data Upload Tool (see page 303)

DBUtil: RiskMinder Database Tool

During RiskMinder installation, the installer collects the information to connect to the RiskMinder database. After the installation is completed, this information is stored in an encrypted format in a file called securestore.enc. This file stores the following encrypted information that you need to connect to the RiskMinder database:

- Database user name and password (Used by RiskMinder Server to connect to the database.)
- Master key (Used for encrypting the database user name and password that is stored in securestore.enc.)

RiskMinder supports both software and hardware modes to protect the data. The DBUtil tool can be used to perform database operations for both the modes.

If for some reason you need to add a new database user name, password, or DSN or change the master key value any time *after* installation, then you can use DBUtil to perform these tasks.

This section includes the following topics:

- Using DBUtil Options (see page 294)
- Updating the Master Key (see page 297)

Note: Because the master key is used for encrypting sensitive information, for security reasons, the DBUtil tool *does not* provide any option to view the key value.

Using DBUtil Options

The following table lists the options for dbutil. In this table, *key-value* pair refers to either DSN, password, or database username/password pair. The DSN/password is used by RiskMinder Server, while user name/password is used by Administration Console and User Data Service.

Important! Because the master key is used for encrypting sensitive information, for security reasons, the DBUtil tool *does not* provide any options to view the key value.

Option	Description
-h	Displays the Help for the tool. Syntax: **dbutil -h**

Option	Description
-init	Creates a new securestore.enc with the new master key that you specify, as discussed in "Updating the Master Key" (see page 297). Syntax: **dbutil -init key** For example: dbutil -init MasterKeyNew dbutil -init RiskFortDatabaseMKNew **Important!** This command succeeds only if there is no securestore.enc in the conf directory.
-pi	Inserts an additional key-value pair into securestore.enc. Syntax: **dbutil -pi <key> <value> [-h HSMPin [-d HSMModule]]** **-h HSMPin** is required if **securestore.enc** is protected by HSM cryptography. **-d HSMModule** is optional when **-h** is present. It defaults to "nfast" (NCipher). For example: dbutil -pi RiskFortBackupDSN dbapassword dbutil -pi Jack userpassword dbutil -pi Jack userpassword -h hsmpassword -d chrysalis **Important!** Each key can have only one value. If you have already inserted a key-value pair, then you cannot insert another value for the same key.
-pu	Updates the value for an existing key-value pair in securestore.enc. This feature can be used when you need to update the database password. Syntax: **dbutil -pu <key> <value> [-h HSMPin [-d HSMModule]]** For example: dbutil -pu RiskFortDatabaseDSN newPassword dbutil -pu Jack userPassword dbutil -pu Jack userpassword -h hsmpassword -d chrysalis

Option	Description
-pd	Deletes the specified key-value pair from securestore.enc. Syntax: **dbutil -pd <key> [-h HSMPin [-d HSMModule]]** For example: dbutil -pd RiskFortDatabaseDSNOld dbutil -pd Jack
-i	Inserts the specified primary name-value pair in securestore.enc, if hardware-based encryption is used to secure the data in this file. This is used during server startup to provide HSM initialization information. Syntax: **dbutil -i <primeKey> <HSMPin>** where *primeKey* is the name of the HSM module. For example: dbutil -i chrysalis hsmpassword
-u	Updates the specified primary name-value pair in securestore.enc, if hardware-based encryption is used to secure the data in this file. Syntax: **dbutil -u <primeKey> <HSMPin>** where *primeKey* is the name of the HSM module. For example: dbutil -u chrysalis newhsmpassword
-d	Deletes the specified primary name-value pair from securestore.enc, if hardware-based encryption is used to secure the data in this file. Syntax: **dbutil -d <primeKey>** where *primeKey* is the name of the HSM module. For example: dbutil -d chrysalis

Updating the Master Key

Specified during installation, the *master key* is used to encrypt the values in the securestore.enc file. It also encrypts all encryption keys that are used by the product and are stored in the RiskMinder database.

If for security reasons you need to change the master key value in securestore.enc, then:

1. Back up the current securestore.enc file.

   The current securestore.enc is available at:

   - **On Windows**
     `<install_location>\Arcot Systems\conf`
   - **On UNIX-based Platforms**
     `<install_location>/arcot/conf`

2. Delete the securestore.enc in ARCOT_HOME\conf.
3. Navigate to the following location where DBUtil is available:

   - **On Windows**
     `<install_location>\Arcot Systems\tools\win`
   - **On UNIX-based Platforms**
     `<install_location>/arcot/tools/<platform_name>`

4. Run the following command:
   `(For software mode) dbutil -init <master_key_name>`
   `(For hardware mode) dbutil -init <HSM_Key_Label>`

   The tool re-creates securestore.enc with the master key name that you specify.

   Important! If the master key setup fails, contact CA Support for help.

5. Update the database information in the securestore.enc file.

   The RiskMinder installer automatically configures the database username/password and database DSN/password information in securestore.enc. However, after creating a new securestore.enc file, you must manually insert this information in the new file. You need to use the dbutil -pi option to do so.

   To insert the supplied database values in securestore.enc, use the following commands:

   - (For software mode) dbutil -pi *<dbUser> <dbPassword>*
   - (For hardware mode) dbutil -pi *<dbUser> <dbPassword> [*-h *HSMPin [*-d *HSMModule]]*

     In the preceding commands, dbUser is the database user name and dbPassword is the password associated with the specified user name. For example:

     dbutil -pi arcotuser welcome123

Note: The user name that you specify in this command is case-sensitive.

- (For software mode) dbutil -pi <*dsn*> <*dbPassword*>
- (For hardware mode) dbutil -pi <*dsn*> <*dbPassword*> *[*-h *HSMPin [*-d *HSMModule]]*

  In the preceding commands, dsn is the data source name and dbPassword is the database password. For example:

  dbutil -pi arcotdsn welcome123

Note: The DSN name that you specify in this command is case-sensitive.

6. If you have performed distributed deployment of RiskMinder, then you must copy the new securestore.enc file to all the systems where RiskMinder components are installed.

arrfversion: RiskMinder Modules Version Display Tool

The arrfversion tool enables you to check and display the versions of *RiskMinder Rule and Plugin modules* (.dll files on Windows and .so on UNIX-based platforms) that are available at the following directories (relative to ARCOT_HOME):

- **/bin/**
- /plugin/**rules/**
- /plugin/rules/**addon/**

When you contact CA Support for problems related to deployment and operation, make it a practice to specify the version of the deployed modules. This helps in faster identification and resolution of a problem.

Syntax:

The syntax to use the tool is:

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

In the preceding syntax, the <*libraryN_path*> string specifies the name of an individual module, such as:

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

If you do not specify the absolute path of the library module, then the specified module is looked up in the folders specified by the standard environment variables. For example:

- %PATH% **for Windows**
- $LD_LIBRARY_PATH **for UNIX-based platforms**

Examples:

- **Windows:**
  ```
  arrfversion ScoreEngine.dll
  ```
- **UNIX-Based Platforms:**
  ```
  arrfversion /opt/arcot/plugins/rules/libaradminprotocol.so
  ```

arrfclient: Server Refresh and Shutdown Tool

The arrfclient tool enables you to gracefully shut down the server or refresh its cache without restarting it. In case of graceful shutdowns, the server allows all existing requests to complete while not accepting any new requests.

Before You Use the Tool

Before you use the tool, you must configure the settings in riskfortadminclient.ini. This file is available at the following location:

On Windows:

`<install_location>\Arcot Systems\conf\`

On UNIX Platforms:

`<install_location>/arcot/conf/`

Note: See "Configuration Files and Options" in the *CA RiskMinder Installation and Deployment Guide* for detailed information on riskfortadminclient.ini.

The minimal parameters in this file that must be configured for the tool to work properly are listed in the following table.

Parameter	Default	Description
Host	localhost	The host name or the IP Address of the system where RiskMinder Server is running.
Port	7980	The port number on which the server is listening to server management requests.
Transport	tcp	The transport mode for server management listener.

These settings ensure the typical TCP-based communication between the tool and RiskMinder Server.

Running the Tool in Interactive Mode

The tool provides the -i option to run it in the interactive mode. When run in this mode, the server starts its own console prompt (#). To run the arrfclient tool in the interactive mode:

1. Navigate to the location where the tool is available:
   - **On Windows:**
     `<install_location>\Arcot Systems\bin\`
   - **On UNIX-based platforms:**
     `<install_location>/arcot/bin/`
2. Run the following command:
   `arrfclient -i`

   The tool starts in interactive mode.
3. Specify the options listed in the following table to perform the required task:

Options	Description
?	Lists the commands for all the options supported by arrfclient.
cr	Refreshes the cache of the server instance. You must enter the instance IP and the server management port number. ■ The instance IP is the IP address or the host name at which RiskMinder Server or Case Management Queuing Server is available. ■ The port number at which RiskMinder Server or Case Management Queuing Server listens to the operations requests. **Note:** By default, RiskMinder Server is available on port 7980. After successful operation, the message "Instance refreshed successfully" and a transaction ID is returned.
sd	Shuts down the RiskMinderFort Server instance. You must enter the instance IP and the server management port number. After successful operation, the message "Successfully initiated shutdown operations" and a transaction ID is returned.
q	Closes the interactive mode.

arrfserver: RiskMinder Server Tool

The arrfserver tool enables you to troubleshoot RiskMinder Server connection errors (for example, if it is not coming up) and allows you to configure the following setting from the command line in interactive mode:

- The authentication and authorization settings for RiskMinder Web services.
- The RiskMinder settings that are either used rarely or are needed only under certain deployment scenarios.
- The RiskMinder configurations that are not exposed through Administration Console.

Running the Tool in Interactive Mode

The tool provides the -i option to run it in the interactive mode. In this mode all the server configurations are done in a similar fashion as that in the service mode, except that the listeners are not started.

When run in this mode, the server starts its own console prompt (#). To run the arrfserver tool:

1. Navigate to the location where the tool is available:
   - **On Windows:**
     `<install_location>\Arcot Systems\bin\`
   - **On UNIX-based platforms:**
     `<install_location>/arcot/bin/`
2. Run the following command:
   `arrfserver -i`

   The tool starts in interactive mode.
3. Specify the options listed in the following table to perform the required task.

Option	Description
?	Lists the commands for the *all* the options supported by arrfserver.
??	Searches the commands based on the pattern you provide. For example, if you enter ?? conf, then all the tool options that match the pattern are displayed.
help	Explains the specified command in more detail. For example, if you enter help setsaconf, then the usage of the command is briefly explained.

Option	Description
setsaconf	Enables you to configure the Web Services APIs that are provided by RiskMinder Server for authentication and authorization. **Note:** Do *not* use this option.This option was used in the previous release to configure the Web services for authentication and authorization. For more information on enabling Web Services for authentication and authorization, see "Configuring Web Services Authentication and Authorization" (see page 53).
q	Closes the interactive mode.

arrfupload: Quova Data Upload Tool

RiskMinder uses Quova data to identify the geolocation information of a user by using the IP address of the system from which the transaction originated. It then uses this data to evaluate Negative Country, Negative IP, and Zone Hopping rules.

See "Configuring Untrusted IP Types" (see page 192), "Uploading List Data" (see page 212), and "Configuring Zone Hopping" (see page 198) for more information. Also, see "Geolocation and Anonymizer Data" (see page 405) for information on how IP geolocation data is used in RiskMinder.

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 information related to geolocation must be downloaded every week, while the data files related to Anonymizer must be downloaded every month. Contact CA Support for the details about the download procedure.

The *Arcot RiskMinder Data Upload Tool* (arrfupload) is a command-line utility that enables you to upload the geolocation data from Quova files to the RiskMinder database.

Before You Use the Tool

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

On Windows:

`<install_location>\Arcot Systems\conf\`

On UNIX Platforms:

`<install_location>/arcot/conf/`

You must configure the parameters in this file (described in the following table) before you can use the tool.

Parameter	Default	Description
Tables	Do Not Load	The tables that the user can work with. Possible values are: ■ GeoPoint ■ Anonymizer
Load	0	The indicator whether to upload the data to the table or not. Possible values are: ■ 0 (Do not load) ■ 1 (Load)
Swap	0	The indicator whether to switch RiskMinder configuration to start using the table where GeoPoint or GeoAnonymizer data has just been uploaded. **Important!** The RiskMinder Server cache must be refreshed after this change. Possible values are: ■ 0 (Do not swap) ■ 1 (Swap)
Filename	--	The name of the file from which the Quova data has to be loaded. **Important!** You must mention the absolute path to the file, along with the file name.

Note: If both, Load and Swap are set to 1, the table is first loaded and then swapped.

Using the Tool

This tool is available at the following location:

On Windows:

`<install_location>\Arcot Systems\bin\`

On UNIX Platforms:

`<install_location>/arcot/bin/`

This tool uses the database information in the arcotcommon.ini file to connect to the RiskMinder database and uses the username and password specified in the securestore.enc file to authenticate to the database.

Syntax:

Run the following command to use the tool:
`arrfupload <option>`

Important! The Quova information that you upload by using this tool is not available until you refresh the RiskMinder Server cache. For instructions on refreshing the cache, see "Refreshing the Cache" (see page 37).

The following table lists the options supported by the utility.

Options	Description
-help	Lists *all* options supported by the tool, followed by the brief usage of the option.

Options	Description
-config	This option is used to read information from riskfortdataupload.ini (the configuration file used by the tool) and perform the required action. This option uses the following flags: ■ Tables**:** The set of tables the user wants to update. The values allowed are either Geopoint or Anonymizer. If neither is specified, then no data is uploaded. This option does not have any default value. ■ Load**:** If set to 1, it indicates that the data will be uploaded and if set to 0, it indicates that data will not be uploaded. The default is value is 0. **Important!** If set to 1, the Filename and Tables flags *must* be set. ■ Swap**:** If set to 1, it indicates that the table will be swapped and if set to 0, it indicates that the table will not be swapped. The default value is 0. **Important!** This flag is valid only if the Tables flag is set correctly. Also, you must refresh the RiskMinder Server cache to use the new table. ■ Filename**:** Indicates the name and the path of the Quova file that contains the data to be uploaded. **Important!** This flag is valid only if the Load flag is set to 1.
-tnames	This option is used to display the current ARQGeoPoint and ARQGeoAnonymizer tables being used by the RiskMinder database.
-prompt	This option is used to display an interactive command-line menu that enables the user to select the table (ARQGeoPoint or ARQAnonymizer) that they want to update by using the latest Quova data. Based on the table specified by the user, a submenu with the following options appears: ■ **Load Quova Data:** Depending on the set of tables chosen from the main menu, this option 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 and the path where this file is available. ■ **Swap Quova Tables:** Depending on the set of tables chosen from the main menu, this option enables the user to swap tables. ■ **Exit to the previous menu:** Enables the user to access the main menu. ■ **Exit the program:** Enables the user to exit from the tool.

Options	Description
-prompt <<*Table name*> <*Load*> <*Swap*> <*Absolute path of the file*>> [<*Table name*> <*Load*> <*Swap*> <*Absolute path of the file*>]	This option is used to set up a scheduled task to upload both GeoAnonymizer and GeoPoint data.

Chapter 15: Managing Cases

Important! In this section, some tasks (Handling Cases (see page 337)) can be performed by Customer Support Representatives, some (Analyzing Transactions (see page 358)) only by Fraud Analysts, and some (Creating a New Queue (see page 329)) by Queue Managers. However, an Organization Administrator (OA) and a Global Administrator (GA) have all the privileges to handle these tasks for the organization(s) in their purview.

The Case Management feature of RiskMinder provides your User Administrators (UAs) and Fraud Analysts (FAs) a single unified view of the data related to cases. This enables them to analyze the data more efficiently and take faster, better-informed decisions towards resolving the cases. In addition, analysts can also constantly track the status and progress of their cases and maintain complete case histories with instant access to all related information.

This feature enables you to:

- Efficiently manage customer service and support
- Manage large numbers of cases and investigations
- Create actions and tasks with due dates
- Assign actions with due dates
- Record investigation notes and the resolution provided to the user
- Handle cases and tasks more efficiently
- Keep clear audit trail or history of actions on a case
- Analyze trends
- Generate fraud-related reports

This section guides you through the basics of RiskMinder Case Management, and covers the following topics:

- Understanding RiskMinder Cases (see page 310)
- Case Roles (see page 318)
- Case States (see page 322)
- Case Management Workflows (see page 324)
- Creating a New Queue (see page 329)
- Managing the Case Queue (see page 330)
- Rebuilding a Queue (see page 336)
- Analyzing Transactions (see page 358)
- Handling Cases (see page 337)
- Generating Case Management Reports (see page 342)

Understanding RiskMinder Cases

The *Case Management* feature enables you to investigate transactions, and intuitively and effectively manage the transactions that are marked suspicious. This feature simplifies the challenge of recording and documenting every phase of an investigation, creating a clear and comprehensive trail of activity. This feature also saves time by automatically creating a report of the findings, including a detailed listing of reason, recommendation, geolocation information, connection details, and risk assessment details.

This section explains the important points related to managed cases (or cases, in short) with the help of the following sections:

- Case Basics (see page 311)
- Case Management Components (see page 312)

Case Basics

The following is a gist of managed cases in RiskMinder:

- All transactions (login, wire transfer, or any transaction that your application is evaluating risk for) for a user that result in the **Deny** or **Alert** advice in the RiskMinder system are considered a *case*.

  In other words, one case can comprise multiple suspicious transactions for a user.

- Every case provides information related to the user, transactions details, and case history.

  In other words, there is a strict 1:1 mapping between a user and open cases. As a result if a case is already open for the user, then a new suspicious transaction is added to the existing case. A new case is *not* created if a user already has a case open.

- At any time, a user can only have one open case in the system.

- At any time, a view into the case from Administration Console shows all the transactions within the case that have not been handled by an administrator and, therefore, their Fraud status is still undetermined.

- After a case is created in the system, it is not allowed to be closed as long as *all* the transactions within the case are not handled (marked as Fraud or Not A Fraud).

  When a Customer Support Representative (CSR) handles all these transactions, they must close the case explicitly. Only then the case is considered to be closed.

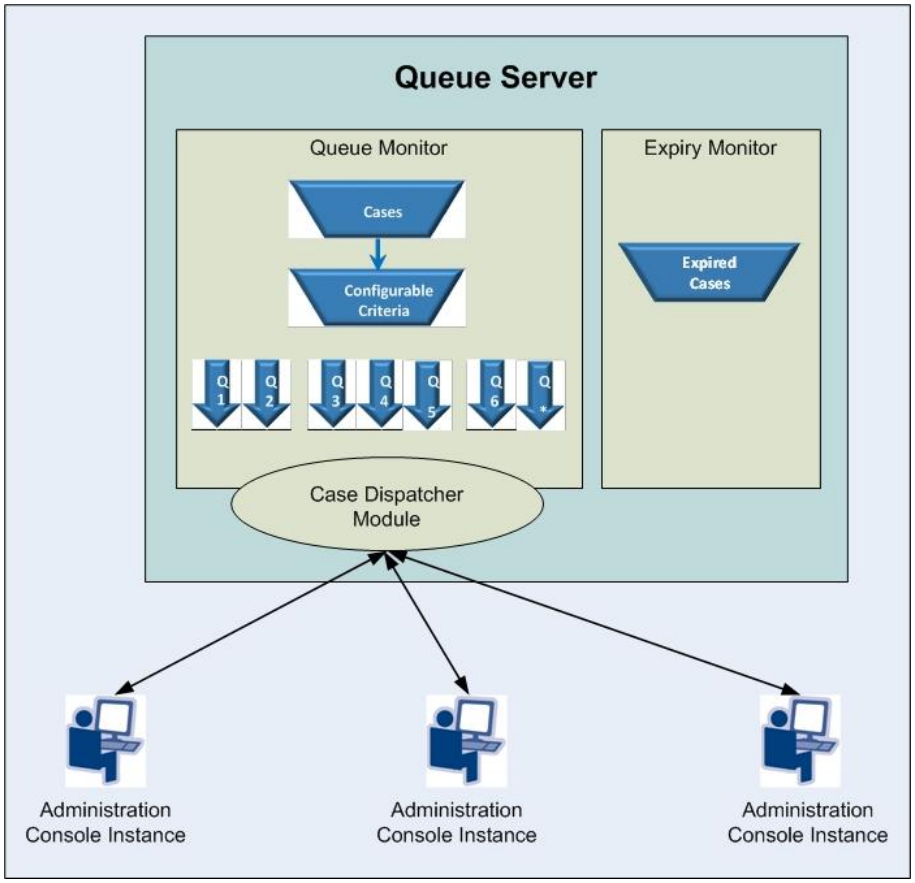
- If a case is closed, then any new warnings or suspect transactions for a given user result in the creation of a new case in the system. All new and future transactions are assigned to this new case.

Case Management Components

The components of the Case Management module include:

- Case Queues (see page 313)
- Queue Server (see page 314)
- Queue Monitor Thread (see page 315)
- Case Dispatcher Module (see page 316)
- Expiry Monitor Thread (see page 317)

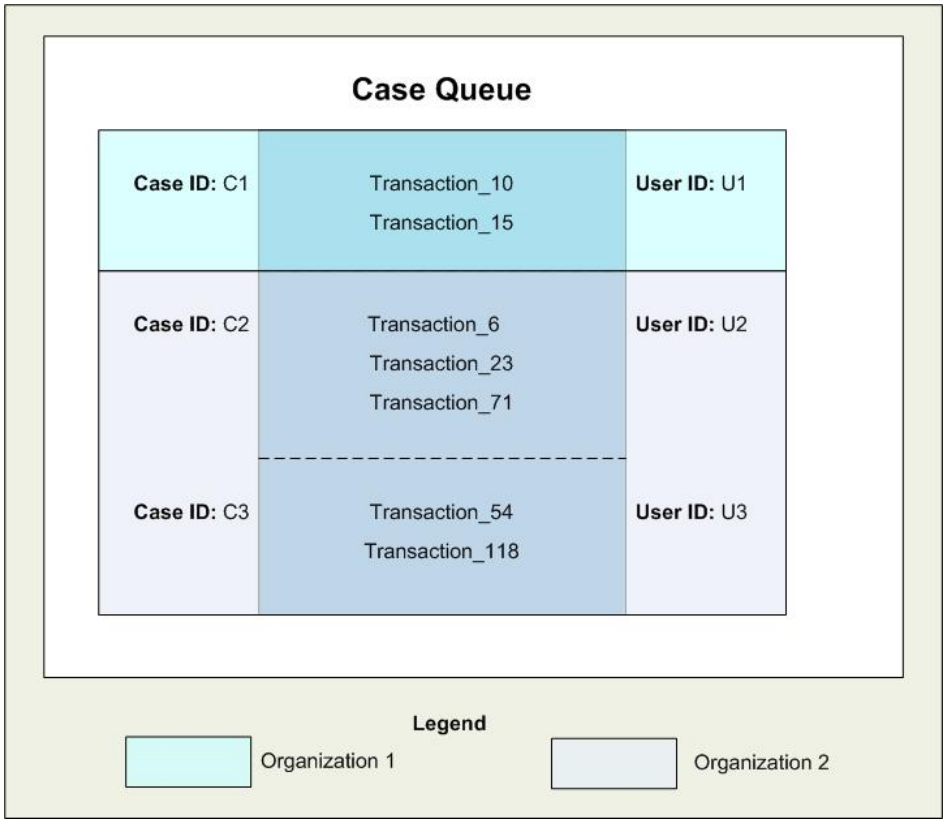
The following figure illustrates how these components work together.



Case Queues

A *Case Queue* (or simply a *Queue*) is a list of cases that are grouped based on criteria, such as **Date Created**, **Date Updated**, **Number of Open Transactions**, and **Next Action Date**. RiskMinder supports multiple Queues for each organization in the system.

The following figure depicts what a typical Queue looks like:



Queues are managed by Queue Managers (see page 320), and are associated with a Queue Name, Case Order criteria in the Queue, and Case Priority. Queue Managers can define a new queue. New cases that are generated are added to the Queue when a Queue rebuild happens. By default, Queue rebuild happens every 30 minutes. The GA can configure this frequency on the Miscellaneous Configuration screen. The Queue Manager for an organization can also issue a Queue rebuild request from Administration Console. Cases that do not fit into any individual Queue are assigned to the DEFAULT queue.

The Queue Manager can assign Customer Service Representatives (CSRs) to work on each Queue, depending upon the skill of the CSR or other organization policies.

Note: More than one CSR can be allocated to a Queue in an organization. Also, if there are multiple organizations in a CSR's purview, the CSR can be allocated to multiple Queues.

Queue Server

The *Queue Server* is responsible for:

- Caching Case Queues (see page 313) and Queue-to-Administrator mapping with the help of the Queue Monitor Thread (see page 315).
- Dispatching the cases in the Case Queues (see page 313) to the active Administration Console instances with the help of Case Dispatcher Module (see page 316).
- Maintaining the updated list of expired cases with the help of Expiry Monitor Thread (see page 317).

Queue Monitor Thread

The *Queue Monitor* (referred to as *Scheduler*) thread runs at the Queue Server (see page 314)-end and is responsible for creating the Case Schedule, populating the Case Queues (see page 313) with cases, and prepares the Queues for Case Dispatcher Module (see page 316).

This thread works as follows:

1. It wakes up at a pre-defined interval and fetches the list of all the latest cases from the database where:
   - At least one transaction shows the Fraud Status as **Undetermined**.

   and

   - The case has not expired.
2. Caches the Queues with cases.
3. Based on the case state and other criteria (such as **Transaction Date**, **Transaction Amount**, or **Next Action Date**), the thread assigns the cases into the Case Queues (see page 313).
4. For more information on case states, see "Case States" (see page 322).
5. When a case is assigned to the Queue, an in-memory list is created for the Queue.
6. On completion of the case assignment to a Queue, the state of all the assigned cases is changed to OPEN.
7. When the Customer Service Representatives (see page 318) (CSRs) click the **Save and Go to Next Case** or the **Go to Next Case** button:
   a. A request to fetch the next case in the Queue is sent to the Queue Monitor Thread (see page 315) via Queue Server (see page 314).
   b. In response, the Case Dispatcher Module (see page 316) picks the case from the memory queue and returns its Case ID to the Administration Console instance from where the request originated.
8. The state of the case is then changed to IN PROGRESS, and the CSRs can work on the case.
9. On receiving the Case ID, the Administration Console instance fetches all the transactions for the case from the database and displays the same to the CSR.

   Based on the case review process, the case state can change. See "Case States" (see page 322) for more information.

Case Dispatcher Module

The *Case Dispatcher Module* (referred to as *Dispatcher*) listens to the case requests from the individual CSRs at the Queue Server (see page 314)-end and "pushes" the cases (as per their order in the Queue) from the Case Queues (see page 313) to the individual Administration Console instances on demand.

This module works as follows:

1. When CSR logs in, a request is sent to the Dispatcher to fetch the next case.
2. The Dispatcher fetches the next case from the Queue(s) assigned to this CSR.
3. The Dispatcher, then, acquires a lock on the selected case in the RiskMinder database.
4. The Dispatcher also changes the status of the case from OPEN to INPROGRESS, and updates the affected table with the name of the CSR from whose Administration Console instance the request originated.
5. The Dispatcher, then, sends the case details back to the Administration Console instance, which then fetches the transactions for the case and displays them on the screen for the CSR.
6. The Administration Console instance also sets a Timeout for the displayed case details.

   This prevents the CSR from opening a case page and then not working on it within the pre-defined time interval. If the current case allocation to the CSR times out, an appropriate message is displayed to the CSR. The case subsequently times out and its status is changed to OPEN.
7. If the currently displayed case does *not* timeout and the CSR moves to the next case in the Queue, the case status is changed from INPROGRESS back to OPEN.

   The CSR can view the next case by clicking the **Go To Next Case** button on their screen.

Expiry Monitor Thread

The *Expiry Monitor* thread is responsible for marking all the cases that have expired since the last time the thread ran. It wakes up at a much lesser frequency than the Queue Monitor Thread (see page 315).

This thread works as follows:

1. It wakes up at a pre-defined and configurable interval and fetches a list of all cases:
   - That are in the OPEN or NEW state.

   and

   - For which the case update time is more than the configured expiration time.

   In other words, it looks for cases that have not been worked upon and for which no new alerts have been generated.
2. Next, the thread updates the status of all cases identified in the preceding step as EXPIRED in the RiskMinder database.
3. The thread goes back to sleep.

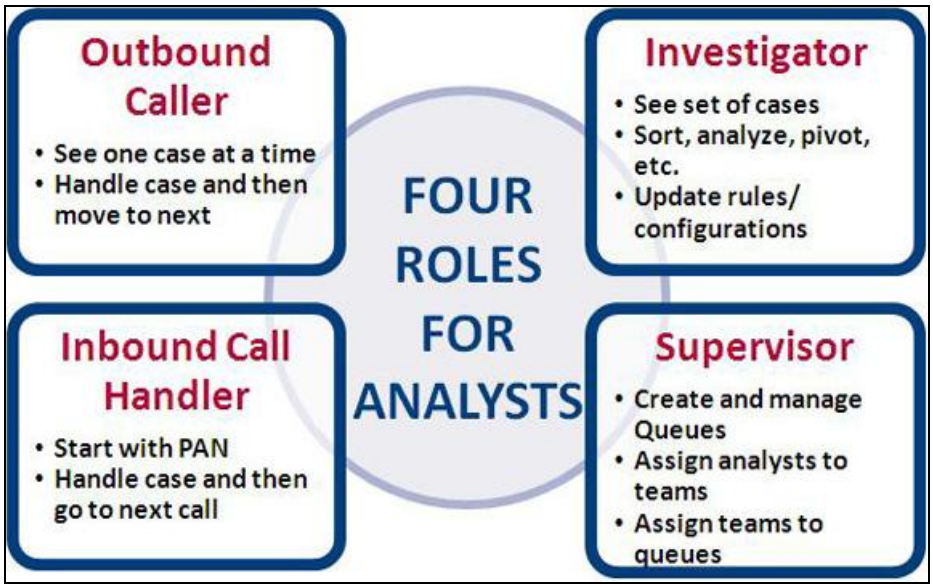
Case Roles

The Case Management feature supports the following broad categories of roles:

- Customer Service Representatives (see page 318)
- Queue Managers (see page 320)
- Fraud Analysts (see page 321)

Subsection, "Case Role Privilege Summary" (see page 321), summarizes the privileges available to these roles.

The following figure shows the different case roles and the tasks performed by each role.



Customer Service Representatives

As the name suggests, *Customer Support Representatives* (CSRs) are your organization's interface with the end user. They are responsible for:

- Working on Cases (see page 319)
- Handling Customer Calls (see page 319)

Working on Cases

They typically review cases that are automatically allocated to them and work on these cases. When they start working on a case, the case is marked with their name. As a result, the case will not show in another CSR's screen. However, the Queue Managers (see page 320) can reassign the case to another CSR by assigning another CSR to the Queue.

CSRs can also call end users to confirm the authenticity of a suspect transaction. Their main activities include:

- If required, call the end users to verify if a transaction is fraudulent or not.
- Add users to the **Exception User List** for a specified duration, based on the user input.

  The default duration is 10 days, but they can change it as required.
- After reviewing a case, CSRs can update the case. As a result of which, they can change the case status from **In Progress** to one of the following:
  - On Hold
  - Closed
- They can also take appropriate notes in a free-form field to capture the progress of the investigation.

Handling Customer Calls

At times, the CSRs also handle incoming calls from the end users. In other words, they attend customer calls. For example, a customer might call the Call Center because they see transactions that they did not perform. In such cases, these operators record the input from the customer, if a case for the specified user already exists. If a case does not exist for the customer, then a case is generated automatically.

Note: The input collected by CSRs is used by the Fraud Analyst for analyses.

In this case, the CSRs:

- Handle user calls.
- Record user inputs.

  They can take appropriate notes in a free-form field to capture the progress of the investigation.
- View recent activities of the user.
- Add users to the **Exception User List** for a specified duration, based on the user input.

  The default duration is 10 days, but they can change it as required.
- Search for the transactions by the user in the given time period.

Queue Managers

Queue Managers (or simply, Supervisors) determine the order in which cases are assigned to the Queue. They can:

- Create new Queues and assign cases to one of several Queues for their organization.

  See "Creating a New Queue (see page 329)" for more information on how to create a Queue.

- Manage the Queues for all organizations in their scope.

  See "Case Queues" (see page 313), for more information on Queues.

- Rebuild a Queue.

  See "Rebuilding a Queue" (see page 336) for more information.

- Assign and reassign CSRs to the Queues in their scope.

Note: By default, Queue Managers *cannot* perform the tasks of a Fraud Analyst. However, you can use **Custom Roles** to create a new role based on Queue Manager and assign the FA privileges to this role. For more information on how to create custom roles, see "Creating a Custom Role" (see page 57).

Fraud Analysts

Fraud Analysts (FAs) research and analyze fraud patterns in transactions to define anti-fraud strategies. They analyze the trends in transactions by using the truth data collected by other CSRs *and* the available filters, such as:

- Transactions by the same user in the given time period.
- Transactions from the same user device in the given time period.
- Transactions from the same IP address in the given time period.

Based on their analyses, FAs can then advise the system administrators on fine-tuning RiskMinder. In addition, if they suspect a transaction to be suspicious, they can raise a request for CSRs to call the end user and find more details related to the suspect transactions, even if the system had not suspected those transactions previously.

The following list describes the main functions performed by Fraud Analysts:

- They can log in and view the list of transactions in real time.
- They can set a combination of filter conditions to view transactions for all users over a period of time for those matching specific risk status values.
- As part of the investigation, the FA can also search for similar transactions. They can define the filter to detect similarity based on:
  - Transactions by the same user in the given time period.
  - Transactions from the same user device in the given time period.
  - Transactions from the same IP address in the given time period.
- If the transaction set is large, they can also export the data offline and then analyze it.
- If they locate suspicious patterns, they can raise alerts on those transactions for further investigation by the CSRs. The "alerted" transactions are automatically added to the case for the user in question.

Note: Fraud Analysts *cannot* update any cases.

Case Role Privilege Summary

The following table summarizes the privileges available to the case roles discussed in the preceding sections.

Privilege	CSR	Queue Manager	Fraud Analyst
Manage Inbound Calls	✓	X	X
Work on Cases	✓	X	X

Privilege	CSR	Queue Manager	Fraud Analyst
Manage Queues	X	✓	X
Rebuild Queues	X	✓	X
View Queue Status	X	✓	X
Analyze Transactions	X	X	✓

Case States

During its lifecycle, a case can progress through the following states:

- New (see page 322)
- Open (see page 322)
- In Progress (see page 323)
- On Hold (see page 323)
- Expired (see page 323)
- Closed (see page 324)

New

When a user transaction results in **Alert** or **Deny** advice, then a new case is created for the user, if a corresponding case does not already exist.

The case remains in the **New** state until a CSR opens it or the case expires.

Open

When a CSR opens a new case assigned to them, the case is activated and its state changes to **Open**. When a case is in the **Open** state, new transactions or events can be added to the case.

Unless the case state is either **On Hold** or **Closed**, every case remains in the **Open** state.

In Progress

While a CSR is working on a case, the case state remains **In Progress**. In other words, when they click the **Cancel** button for the current case or click the **Go To Next Case** button to move to the next case assigned to them, the currently open case state changes to **Open**, or to the state that they explicitly changed the case to.

Note: A CSR and Queue Manager can change the status of a case from **On Hold** to **In Progress**.

On Hold

When a CSR postpones the further investigation of a case by specifying the **Next Action Date** for an **In Progress** case, the case state changes to **On Hold**.

Note: All events that are generated within the time frame of **Next Action Date** are appended to the case.

When the specified **Next Action Date** arrives, the case state automatically changes to **Open**.

Expired

When no CSR works on a **New** case within a pre-defined number of days, the case state changes to **Expired**.

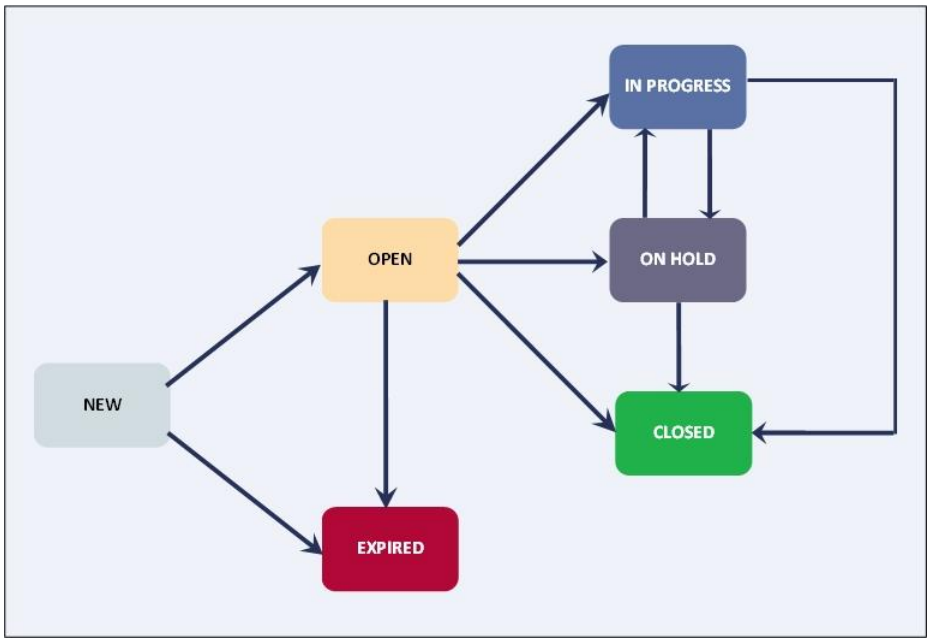
Note: The time the last transaction was added to the case or was updated is considered as the *Starting Date* for the case. The case *Expiration Date* is calculated as the Starting Date + *N* days, where *N* is a configurable value. The default value for *N* is **10 days**.

New transactions cannot be added to an expired case. A new case (and therefore a new Case ID) is created, and the new transactions or events are added to this new case.

Closed

When a CSR resolves an **Open** case and explicitly marks it as **Closed**, the case state changes to **Closed**.

The following figure illustrates how the states of a case change.



Case Management Workflows

This section covers the workflows for the following phases in the lifecycle of a case:

1. Case Generation (see page 325)
2. Case Queuing (see page 325)
3. Case Assignment (see page 326)
4. Case Handling (see page 327)
5. Case Expiry (see page 327)
6. Fraud Analysis (see page 328)

Case Generation

Typically, cases are created automatically by the system. However, if a case operator manually flags a suspicious transaction for a user, or a Fraud Analyst discovers a suspicious pattern in user transactions, then they can add the suspicious transactions to the case.

A case is generated when:

- The advice for the risk evaluation for a transaction is either **Alert** or **Deny**.

  Note: If a case is already open for the user, then this transaction is added to the existing case. You can configure this on the Miscellaneous Configurations page.

- A user contacts your Call Center to dispute a transaction.

  In this case, the case operator can either refer the disputed transactions for further investigation or can mark the transaction as a fraud. In both the cases, the transaction is automatically added to a case.

- A Fraud Analyst suspects some transactions to be fraudulent (typically, based on patterns detected earlier) and marks them for further investigation.

  Note: These transactions are then added to the existing case.

Case Queuing

When a case is created and transactions are added to the case, the cases need to be assigned to the Queue that belongs to the organization. In addition, CSRs who can work on these cases must also be assigned to each Queue. The Queue Monitor Thread (see page 315) plays the pivotal role in this case.

See "Queue Monitor Thread" (see page 315) for detailed information on how this thread queues cases.

Case Assignment

After a case has been queued, it then needs to be dispatched to each CSR's screen. The Case Dispatcher Module (see page 316) plays the pivotal role in this case.

See "Case Dispatcher Module" (see page 316) for detailed information on how this thread dispatches cases.

Notes Related to Case Assignment

Some points to remember on this topic are:

- A new case is assigned to a CSR from the organization to which the case belongs.
- The cases are assigned based on their order in the Case Queue. The order criteria can include:
  - Next Contact/Action Date
  - Number of open transactions in the case
  - Age of the case (Date Created)
  - How long ago the case was last updated
- Every case is eventually handled by a CSR in an organization.

Case Handling

Cases are handled by the CSRs as follows:

- A new transaction flagged by the FA or a Deny or Increase Authentication advice generated for a transaction creates a new case. The status of the case *before* the Queue Monitor Thread (see page 315) schedules it is **NEW**. The Queue Monitor Thread (see page 315) changes it to **OPEN**, and when a CSR finally views the case, the case status is changed to **INPROGRESS**.

  Note: Even before the case is handled by a CSR, more flagged transactions might be added to the case.

- A CSR is automatically assigned to work on the case.
- Contact the user out of band, say by sending an email or by calling them on the specified contact number.
- Based on the ongoing investigation and the results of contacting the end user, the CSR can update the case, as it develops:
  - Search for transactions based on a specific time interval.
  - During the user interaction, add previously unsuspected transactions to the case.
  - Choose resolutions for one or more of the transactions in the case.
  - Mark the case for follow up and set the **Next Action Date**.

    Typically, the **Case Status** of such cases is then updated to either **INPROGRESS** or **ONHOLD**, and the user is contacted by a CSR later.
  - Based on user input, add the user to the **Exception User List** for a specified period of time.
  - Resolve the case and change the **Case Status** to **CLOSED**.
- The Queue Managers (see page 320) can also reopen an expired case, if required.

Case Expiry

A case can expire if all of its transactions are not handled within the stipulated amount of time or if there is no activity on the case for a pre-defined time period.

Note: The default case expiry time is 48 hours.

See "Expiry Monitor Thread" (see page 317) for detailed information on how this thread manages expired cases.

Fraud Analysis

The gist of the fraud analysis workflow for transactions by Fraud Analysts (see page 321) is as follows:

- FAs can search for transactions based on criteria, such as Transaction Date, Secondary Authentication Status, Transaction type, Risk Advice and Case Status. For more information, see "Step 1: Viewing Transactions Summary" (see page 359):
  - All transactions are initially shown in the Transaction Summary view.
  - Initially, all transactions have the Case Status of **New**.
  - The list of transactions can be exported to a .csv file for processing in Microsoft Excel.
- The FAs can click a case to view its details. For more information, see "Step 2: Viewing Case Details" (see page 362).
- The FAs can also search for all transactions that are similar to a case. For more information, see "Step 3: Viewing Similar Transactions" (see page 368).
- If they find suspect transactions and potential fraud patterns during their analyses, FAs can mark the transactions for further investigations by CSRs. For more information, see "Step 4: Marking Transactions for Further Investigation" (see page 369).

Creating a New Queue

Important! Only a GA, an OA, or a Queue Manager (QM) can perform the tasks (for the organizations that are in their scope) described in this section. The MA, UAs, FAs, and CSRs *cannot* perform these tasks.

A Queue Manager can create a new Queue by specifying the name, description, criteria, and priority for the queue. The Queue Manager also assigns administrators to a Queue. An administrator can be assigned to multiple Queues, and multiple administrators can be assigned to the same Queue.

To create a new Queue:

1. Log in to Administration Console as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, specify the Organization for which you want to create a Queue.
5. The updated page appears.
6. Click **Create New Queue**.

   The updated page appears.
7. Specify the **Queue Name**.
8. Specify a **Display Name** for the queue.
9. Specify the **Queue Description**, if required.
10. In the **Assign Administrators** section:
    a. From the **Administrators** list, select the required administrators that you want to assign to the queue.
    b. Click the **>** button to move the selected administrators to the **Selected Administrators** list.

    Note: If you want to move all the **Administrators** to the **Selected Administrators** list, then click the **>>** button to do so.
11. In the **Criteria** section:
    a. Define the criteria (**Risk Advice** or **Matched Rule**) to determine which cases are added to the queue.
    b. Select the operator and value from the corresponding drop-down lists.
    c. Click **Add** to add the expression to the expression area.
    d. Use the AND, OR, (, or) operators to combine fragments and build the final criteria expression.

Cases that match this expression will be assigned to the queue you create.

12. In the **Order By** section:
    a. Specify the element by which you want to sort the Queue. The options available are:
        - Next Contact Date
        - Date Created
        - Date Updated
        - Number of Open Transactions
        - Risk Advice
        - Risk Score
    b. Specify the order by which you want to order the corresponding element. The options available are:
        - Ascending
        - Descending
13. Click **Save** to save the updates you made on the screen and create the Queue.
14. Refresh the organization cache for the changes to take effect.

    See "Refreshing Organization Cache" (see page 253) for detailed information on how to do this.

Managing the Case Queue

Important! Only OAs, GAs, or Queue Managers (QMs) can perform the tasks (for the organizations that are in their scope) in this section. The MA, UAs, FAs, and CSRs *cannot* perform these tasks.

This section walks you through the following tasks related to Case Queue management:

- Viewing the Status of the Queue (see page 331)
- Updating the Status of the Queue (see page 332)
- Disabling the Queue (see page 333)
- Enabling the Queue (see page 334)
- Deleting the Queue (see page 335)

Viewing the Status of the Queue

On the Queue Status page, you can view the latest statistics related to the **DEFAULT** Queue. The statistics you can view are:

- Total Open Cases
- Total Diarized Cases
- In-Progress Cases
- Total Cases
- Number of Administrators Assigned

It also shows the details of the **Cases Handled in Last 8 Hours**.

To view the Queue Status:

1. Log in to Administration Console with the necessary privileges to manage Queues.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **View Queue Status** link to display the Queue Status page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to view.

   The page with the updated Queue details appears.

Note: Diarized cases (not in queue) appear separately along with **Inbound Cases (In-Progress)**.

Updating the Status of the Queue

You can update the status of the Queue by using any one of the following methods:

- By clicking the **View Queue Status** link to display the corresponding page, and then clicking the link in the **Queue Name** column corresponding to the queue you want to update.
- By using the **Manage Queues** link under the **Queue Management** section.

To update the status of the Queue by using the latter option:

1. Log in to Administration Console with the necessary privileges to manage Queues.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to update.
5. From the **Queue Name** list, select the name of the queue you want to manage.

   The updated page appears.
6. Specify the **Queue Description**, if required.
7. In the **Assign Administrators** section:
   a. From the **Administrators** list, select the required administrators that you want to assign to the queue.

      Note: To select more than one administrator, press the SHIFT key and click the required administrators.

   b. Click the **>** button to move the selected administrators to the **Selected Administrators** list.

      Note: If you want to move all the **Administrators** to the **Selected Administrators** list, then click the **>>** button to do so.
8. (If you chose a Queue other than DEFAULT Queue) In the **Criteria** section:
   a. Define the criteria (**Risk Advice** or **Matched Rule**) to determine which cases are added to the queue.
   b. Select the data item, operator, and value from the corresponding drop-down lists to define the criteria.
9. In the **Order By** section:
   a. Specify the element by which you want to sort the Queue. The options available are:
      - Next Contact Date
      - Date Created
      - Date Updated

- Number of Open Transactions
- Risk Advice
- Risk Score

b. Specify the order (**Ascending** or **Descending**) by which you want to order the corresponding element.

10. Click **Save** to save the updates you made on the screen.
11. Refresh the organization cache for the changes to take effect.

    See "Refreshing Organization Cache" (see page 253) for detailed information on how to do this.

Disabling the Queue

Note: To be able to disable a Queue, you must ensure that you have the appropriate privileges and scope to do so. Only GAs, OAs, and QMs can disable Queues.

To disable a Queue:

1. Log in as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to update.
5. From the **Queue Name** list, select the name of the queue you want to disable.

   The updated page appears.
6. Click **Disable This Queue** to disable the queue.
7. Refresh the organization cache for the changes to take effect.

   See "Refreshing Organization Cache" (see page 253) for detailed information on how to do this.

Important! You cannot disable the DEFAULT Queue.

Enabling the Queue

Note: To enable a Queue, you must ensure that you have the appropriate privileges and scope. Only the GAs, OAs, and QMs can enable Queues.

To enable a Queue:

1. Log in as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Manage Queues** link to display the Manage Queues page.
4. From the **Select Organization** list, select the Organization whose Queue Status you want to update.
5. From the **Queue Name** list, select the name of the queue you want to enable.

   The updated page appears.
6. Click **Enable This Queue** to enable the queue.
7. Refresh the organization cache for the changes to take effect.

   See "Refreshing Organization Cache" (see page 253) for detailed information on how to do this.

Deleting the Queue

Note: Before you delete a Queue, it is highly recommended that you edit the Queue definition such that no cases are present in this Queue, refresh the cache, rebuild the Queue, and then delete this queue. This ensures that cases, which were in this queue, are not lost.

1. Log in as an OA or a QM.
2. Activate the Case Management tab.
3. Under the Queue Management section, click the Manage Queues link to display the Manage Queues page.
4. From the Select Organization list, select the Organization whose Queue Status you want to update.
5. From the Queue Name list, select the name of the queue you want to delete.

   The updated page appears.
6. Click Delete This Queue to delete the Queue.
7. Refresh the organization cache for the changes to take effect.

   See "Refreshing Organization Cache" (see page 253) for detailed information on how to do this.

Important! You cannot delete the DEFAULT Queue.

Rebuilding a Queue

The Case Management Queuing Server rebuilds the Queues at pre-configured intervals. The default value is 1800 seconds. The GA can change this value at the global level for all organizations by configuring the **Frequency of Automatic Queue Rebuild Schedule (in Seconds)** parameter in the Miscellaneous Configurations page.

There may be a need to rebuild a Queue before the automatic rebuild time in the following cases:

- A new Queue is defined.
- One or more Queue definitions have changed.
- When a Queue has been enabled, disabled, or deleted.

In such cases, the Queue Manager can rebuild the queue using the Rebuild Queues page.

To rebuild a Queue:

1. Log in as a GA, an OA, or a QM.
2. Activate the **Case Management** tab.
3. Under the **Queue Management** section, click the **Rebuild Queues** link to display the Rebuild Queues page.
4. Do one of the following:
   - Select **All Organizations** if you want the QM to rebuild the queues for all organizations in their purview.

     or
   - Select the required organizations from the **Available Organizations** list and click the **>** button to add these organization to the **Selected Organizations** list.

     The **Available Organizations** list displays all the organizations that are available in the scope of the logged in administrator. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.
5. Click **Rebuild** to rebuild the Queue for the selected organizations.

Handling Cases

Important! Only the OAs and CSRs can work on cases that belong to the organizations that are in their scope. The MA, GAs, UAs, and FAs *cannot* perform these tasks.

This section walks you through the following tasks that are related to handling cases and direct interaction with end users:

- Working on Cases (CSRs) (see page 337)
- Managing Inbound Customer Calls (CSRs) (see page 341)

Working on Cases (CSRs)

When RiskMinder marks a transaction as suspect or an FA marks a transaction for further investigation, the case *automatically* appears in the CSR's case list.

To work on the cases in your list:

1. Log in as a CSR.
2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Work On Cases** link.

   The first case (in the order of the priority assigned to your cases) appears.

   The fields in the page are explained in the following table.

Field	Description
User Name	The name of the user who is calling in.
Next Action Date	The date when the user must be contacted the next time.
Case History	The latest case Notes and Additional Notes entered by the previous call handler. If you want to review all the previous notes in this field, then click the **More...** link to do so.
Alerts on This Case	

Field	Description
Mark Selected As	The Fraud Status of the transaction. The possible values in this field are: ■ Undetermined ■ Confirmed Fraud ■ Confirmed Genuine ■ Assumed Fraud ■ Assumed Genuine If you have more than one alerted transaction that need your attention *and* after talking to the user you determine that all of their Fraud Status is the same (say Confirmed Fraud or Confirmed Genuine), then you can use this drop-down list to set the same in one action.
Fraud Status	Based on the previous entry in the Mark Selected As field, this field can have one of the following statuses: ■ Undetermined ■ Confirmed Fraud ■ Confirmed Genuine ■ Assumed Fraud ■ Assumed Genuine
Country	Based on the IP Address, the country from which the transaction was performed.
IP Address	The IP address of the system or device used for the user transaction.
Merchant	The merchant involved in the transaction.
Currency	The currency used in the transaction.
Amount	The total transaction amount.
Matched Rule	The rule that matched and for which RiskMinder flagged the transaction as risky.
Transaction Date	The timestamp when the given transaction was performed.

Field	Description
Risk Advice	The action suggested by RiskMinder after evaluating the Risk Score of the given transaction. The possible actions are: ■ ALLOW ■ ALERT ■ DENY ■ INCREASE AUTHENTICATION
Model Score	The risk score returned by the Model for the transaction.
Secondary Auth Status	If the Risk Advice is INCREASE AUTHENTICATION, then this column specifies the result of the additional authentication that your application returned as feedback to RiskMinder.
Transaction Status	Status of the transaction.
Device Type	The type of device involved in the transaction
Transaction ID	The unique system-generated identifier for the user transaction. **Note:** If required, you can click the Transaction ID to view its details.
OS	The operating system on the device that was used to perform the transaction.
Browser	The browser that was used to perform the transaction.
Device ID Status	The status of the Device ID: ■ **READ**: The Device ID was read from the device. ■ **NEW**: The Device ID was assigned to the device. ■ **REVERSE LOOKUP**: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.
Action	The type of transaction performed by the user, which can be: ■ Login ■ Wire Transfer ■ Any other value that you specify through your application

Field	Description
Channel	The channel on which the transaction was performed.
From To	The pre-defined date range using which you want to filter the data.
Show Transactions	The button to display the alerted transactions based on the preceding From and To fields.
Hide Transactions	The link to hide the displayed alerted transactions.
Case Status	The current status of the case. The possible values are: ■ INPROGRESS ■ ONHOLD ■ CLOSED
Queue	The Queue to which this case has been assigned.
Note	The pre-determined reason for the update.
Additional Note	Any additional information (in addition to the preceding Note) that describes the reason for the change in the case status or any of the fields before. **Important!** This field *cannot* accept more than 250 characters.
Next Action Date (GMT)	The date when the user must be contacted the next time for additional follow-up.
Add User to Exception List	If based on user inputs, you want to temporarily exclude a user from risk evaluation for a specified time interval. For example, a user is travelling to a Negative Country and you do not want the user to be denied any transaction for the same. In this case, you can add the user to the Exception User List. If the user is found in the Exception User List, then by default RiskMinder returns a low Score and the ALLOW advice for transactions originating from these users.
From To	The date range for which you want the user to be exempted from RiskMinder risk evaluation.
Reason	The reason for which the user is being added to the Exception User List.

1. Perform the required actions to capture the user inputs by using the fields explained in the table in the previous step.
2. When done, click one of the following buttons on the page:
   - **Save** to update your changes to the case.
   - **Save and Go To Next Case** to update your changes to the case and go to the next case assigned to you.
   - **Go To Next Case** to go to the next case assigned to you without saving the changes.
   - **Cancel** to cancel any changes you just made on the page.

Managing Inbound Customer Calls (CSRs)

When an end user calls your Customer Support Center to dispute a transaction, then the attending CSR must use the Manage Inbound Calls page to capture the information provided by the user and make the required changes to the case based on this information.

To make the required changes to the case by using the Manage Inbound Calls page:

1. Log in as a CSR.
2. Activate the **Case Management** tab.
3. Under the **Case Management** section, click the **Manage Inbound Calls** link to display the Manage Inbound Calls page.
4. From the **Select Organization** list, select the required organization.

   The updated Manage Inbound Calls page appears.
5. **Enter User Identification** and click **Submit**.

   If you have configured accounts for the organization, you will be prompted to enter the user identifier. You can filter based on user name or the account type from the drop-down list.

   The Manage Inbound Calls page is refreshed with the specified user's case information.

   The fields in the page are explained in the table in Working on Cases (CSRs) (see page 337).
6. Perform the required actions to capture the user inputs by using the fields explained in the table in Working on Cases (CSRs) (see page 337).
7. When done, click **Save** to update your changes to the case.

   If you do not want to save the changes you just made, click **Cancel**.

Generating Case Management Reports

The Case Management module supports the reports explained in the following table.

Report	Description	Case Roles Who Can Generate the Report
Case Activity Report (see page 342)	Displays the cumulative count of all cases that were opened, closed, or were acted upon (any other activity that was performed on cases) in a specified period of time. **Note:** This report is sorted by the Queues to which the individual cases belong, and by the CSR who worked on the cases.	■ Global Administrators ■ Organization Administrators ■ Queue Managers
Average Case Life Report (see page 343)	Displays the statistics related to how long an average case lives in the system. In other words, it summarizes how much activity a case worker expends on a typical case. This report also displays how many cases were closed automatically because they timed out.	■ Global Administrators ■ Organization Administrators ■ Queue Manager

The following subsections explain the fields in these reports and walk you through the steps to generate these reports.

Case Activity Report

The Case Activity Report displays information related to the overall activity on cases in the system, as explained in the following table.

Field	Description
Cases Handled Through	Specifies the Queue to which the case belongs. Typically, these cases are handled by Customer Service Representatives (see page 318) Working on Cases (see page 319).

Field	Description
	The entries in the **Inbound Calls** row summarize the activity details for cases that were handled by Customer Service Representatives (see page 318) Handling Customer Calls (see page 319).
Period	Indicates the period for which the report was generated. This report can be generated for the following periods: ■ By Month ■ Last 7 Days ■ Yesterday ■ By Date Range **Note:** You can see the day-to-day activity details for the period you specified by clicking the button.
Cases Opened	Indicates the total number of new cases that were opened in the specified Period.
Cases Closed	Indicates the total number of existing cases that were closed in the specified Period.
Case Activity Count	Indicates the total number of activities that were performed on the cases in the specified Period.

Average Case Life Report

The Average Case Life Report displays information related to the average time it takes for a case to close in the system, as explained in the following table. These cases are grouped based on the fact whether the cases were closed manually (by a case worker) or automatically, through aging.

Field	Description
Cases Handled Through	Specifies the Queue to which the case belongs. Typically, these cases are closed: ■ By Customer Service Representatives (see page 318) or ■ Automatically, because they timed out

Field	Description
	The entries in the **Inbound Calls** row summarize the activity details for cases that were handled by Customer Service Representatives (see page 318) Handling Customer Calls (see page 319).
Period	Indicates the period for which the report was generated. This report can be generated for the following periods: ■ By Month ■ Last 7 Days ■ By Date Range
Cases Closed	Indicates the total number of existing cases that were closed in the specified Period.
Case Activity Count	Indicates the total number of activities that were performed on the cases in the specified Period.
Average Time Required for Case Closure	Indicates the average time taken to close the cases in the system.

Generating a Case Management Report

Important! Only GAs, OAs, and Fraud Analysts (FAs) can generate this report for the organizations that are in their scope. The MA, UAs, and CSRs *cannot* generate this report.

To generate a Case Management report:

1. Ensure that you are logged in with proper credentials. See the table in Generating Case Management Reports (see page 342) for a summary of the case roles who can generate the corresponding reports.
2. Activate the **Case Management** tab in the main menu.
3. Under the **Case Management** section, click the required link:
   - **Case Activity Report**
   - **Average Case Life Report**
4. Select the required organization for which you want to generate this report from the **Organization Name** list.
5. Depending on the report, additionally you might have to specify the following criteria, as applicable, to view the report:
   - The **Date Range** from the drop-down list.

     or
   - A pre-defined date range in the **From** and **To** fields.
6. Click **Display Report** to view the generated report.

   The required report appears.
7. Click **Export** to save the report to a file or click **New Report** to generate a new report by specifying different criteria.

Chapter 16: Managing Reports

Reports provide the business intelligence that you need to manage your end users and research high-risk events. If you use RiskMinder Case Management, reports help you manage your fraud agents and case activity. "Summary of Reports Available to Administrators" (see page 347) provides an at-a-glance summary of all reports that are available to the different administrators in a tabular format. The sections following the table in Summary of Reports Available to Administrators (see page 347) explain these reports:

- Administrator Reports (see page 350)
- RiskMinder Reports (see page 356)
- Case Management Reports (see page 377)

Reports available through the Administration Console are generated based on the parameters (or filters) that you specify. As a result, you can control the output of a report based on values that you set when you run the reports. The parameters that you can use to filter data include:

- Date Range
- Administrator Name
- Organizations
- User Name

"Generating Reports" (see page 378) walks you through the generic process to generate activity reports for administrators and RiskMinder-specific reports.

You can also export all generated reports to a local file. See "Exporting Reports" (see page 380) for instructions to do so.

Summary of Reports Available to Administrators

The following table summarizes the reports in all categories (Administrator Reports, RiskFort Reports, and Case Management Reports) that are available to all administrators in the system. These reports are then covered in detail in the following sections.

	Report Category		
Administrator	**Administrator Reports (see page 350)**	**RiskFort Reports (see page 356)**	**Case Management Reports (see page 377)**

Administrator	Report Category		
	Administrator Reports (see page 350)	**RiskFort Reports (see page 356)**	**Case Management Reports (see page 377)**
Master Administrator	My Activity Report	Instance Management Report	
	Administrator Activity Report		
	Organization Report		
Global Administrators	My Activity Report	Analyze Transactions Report	Case Activity Report
	Administrator Activity Report	Risk Evaluation Detail Activity Report	Average Case Life Report
	User Activity Report	Risk Advice Summary Report	
	User Creation Report	Fraud Statistics Report	
	Organization Report	Rule Effectiveness Report	
		False Positives Report	
		Device Summary Report	
		Exception User Report	
		Rule Configurations Report	
		Rules Data Report	

Administrator	Report Category		
	Administrator Reports (see page 350)	RiskFort Reports (see page 356)	Case Management Reports (see page 377)
Organization Administrators	My Activity Report	Analyze Transactions Report	Case Activity Report
	Administrator Activity Report	Risk Evaluation Detail Activity Report	Average Case Life Report
	User Activity Report	Risk Advice Summary Report	
	User Creation Report	Fraud Statistics Report	
	Organization Report	Rule Effectiveness Report	
		False Positives Report	
		Device Summary Report	
		Exception User Report	
		Rule Configurations Report	
		Rules Data Report	
User Administrators	My Activity Report	Analyze Transactions Report	
	Administrator Activity Report	Risk Evaluation Detail Activity Report	
	User Activity Report	Risk Advice Summary Report	
	User Creation Report	Fraud Statistics Report	
		Rule Effectiveness Report	
		False Positives Report	
		Exception User Report	

Administrator	Report Category		
	Administrator Reports (see page 350)	**RiskFort Reports (see page 356)**	**Case Management Reports (see page 377)**
Fraud Analysts	My Activity Report	Fraud Statistics Report	
	User Creation Report	Rule Effectiveness Report	
		False Positives Report	
Customer Support Representatives	My Activity Report	Exception User Report	
	User Creation Report		

The following sections explain these reports in detail.

Administrator Reports

In RiskMinder terminology, an *administrator* is someone who has the ability to log in to the Administration Console. Administrators then use reports to audit the activities they perform and the administrators in their purview perform. You access these reports from the **Administrator Reports** submenu under the **Reports** main menu.

Note: See "Elements of the Administration Console" (see page 15) to understand the layout of Administration Console, and how you access this main menu and the submenus under it.

All Administrator reports available in this category include:

- My Activity Report (see page 351)
- Administrator Activity Report (see page 352)
- User Activity Report (see page 353)
- User Creation Report (see page 354)
- Organization Report (see page 355)

My Activity Report

This report lists all operations performed by the current administrator. You use this report to list the actions and operations you have performed for the defined data range.

The following table explains the fields of this report.

Report Field	Description
Date	The date and time when the event was performed.
Administrator ID	The name of the administrator who is generating the report.
Administrator Organization	The name of the organization to which you are currently logged in as an administrator.
Transaction ID	The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to RiskMinder Server. **Note:** You can use this ID to isolate information about a specific transaction in the log files.
Event Type	The type of administrator activity (such as, administrator login, view records, and update user and organization information) that you performed. Some possible event types are: ■ Search Users ■ Search Organization ■ Admin Login ■ Update AdminProfile ■ Set Preferred Locale ■ Create Organization ■ Create Ruleset ■ Create AccountType ■ Get AccountType Details ■ System and Organization Cache Refresh ■ Migrating to Production ■ View Report: *<report name>* ■ Export Transaction Summary ■ Update Global Password Policy ■ Session Expired ■ View Queue Status

Report Field	Description
Status	The status of the transaction: ■ **Success**: If the action was completed successfully. ■ **Failure**: If the administrator failed to complete the action.
Reason	The reason why the transaction failed.
User ID	If the transaction involved modification of user attributes, then this field specifies the name of the user whose attributes were updated or modified.
Target Organization	The name of the organization on which the activity was performed.
Component	The system resource that was used to perform the task. The column values can be: ■ Administration Console ■ RiskFort ResourcePack
Session ID	The unique numerical identifier created each time you log in to Administration Console. This session lasts until you log out.
Instance ID	If there are multiple instances of RiskMinder Server are running, then this field uniquely identifies the instance that you logged in to. **Note:** This data is used by CA Support personnel to diagnose problems.

Administrator Activity Report

This report lists all activities performed by a specified administrator, or by all administrators from a specified organization. Typically, Global Administrators use this report to monitor activity across organizations, while Organization Administrators use this report to monitor the activity with in their organizations.

By using this report, administrators can view the activity in its entirety or drill down to a single administrator.

This report is most useful for Organization Administrators in managing the activity of their administrative team. It includes information, such as administrator login and logout timestamps, organization search, administrator account updates, and related details.

The fields of this report are the same as those of My Activity Report. See the table in My Activity Report (see page 351) for more information on the field details.

User Activity Report

A *user* is a generic term for an end user if RiskMinder is assessing risk in an Enterprise, eBanking, or ePortal application, or for a card holder in the case of an eCommerce and 3D Secure application.

The User Activity Report specializes in the reporting of activities performed on user attributes, which include creating users, updating users, setting Personal Assurance Messages (PAMs), deleting users, updating user status, and authenticating users.

The report contains details, such as user name, status of the user, type of operations performed, and also the IP address of the user system. Therefore, it is most applicable in the Enterprise or ePortal applications, where users are explicitly created by administrators before they are allowed access to protected resources. It is less applicable in case of eCommerce applications, where users are typically auto-created. Although it reports the type of activity, it gives you an idea of the rate of first-time transactions from cardholders.

To generate this report, you must specify:

- The **Date Range**.
- (Optional) The **User Name**.
- The required **Organization Name**.

The following table explains the fields of this report.

Report Field	Description
Date	The date and time when the event was performed.
User ID	The name of the user whose attributes were updated or modified.
Account Type	The account type associated with the organization to which the user belongs.
Account ID	The account ID of the user.
Event Type	The type of administrator activity (such as, administrator login, view records, and update user and organization information) that you performed.
Organization	The organization name to which the user belongs.
Status	The status of the operation: ■ **Success**: If the operation was completed successfully. ■ **Failure**: If the user failed to complete the operation.

Report Field	Description
Transaction ID	The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to RiskMinder Server. **Note:** You can use this ID to isolate information about a specific transaction in the log files.
Reason	The reason why the Operation failed.
Client IP Address	The IP address of the end user's system.
Caller ID	The unique identifier set by the calling application. **Note:** The Caller ID can be blank if the calling application did not set the value.

User Creation Report

The User Creation Report displays details of the users created in the RiskMinder system.

To generate this report, you must specify:

- The **Date Range**.
- (Optional) The **User Name**.
- The required **Organization Name**.

The following table explains the fields of this report.

Report Field	Description
Date Created	The date and time when the user was created.
User ID	The name of the user who was created.
Organization	The organization name to which the user belongs.
User Status	The status of the user: ■ **Active**: If the user is an active user. ■ **Inactive**: If the user is deactivated. ■ **Initial**: If the user is created, but not yet activated.
First Name	First name of the user.
Middle Name	Middle name of the user.
Last Name	Last name of the user.
Email Address	Email address of the user.

Report Field	Description
Telephone Number	Phone number of the user.

Organization Report

This report provides the details of all operations performed on the specified organization. Irrespective of any rules and configurations, this report displays *all* the activities in the organization under the administrator's purview.

To generate this report, you must specify:

- The **Date Range**.
- The **Organization Name**.

The following table explains the fields of this report.

Report Field	Description
Date	The date and time when the activity was performed.
Administrator ID	The name of the administrator who performed the activity.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to RiskMinder Server. **Note:** You can use this ID to isolate information about a specific transaction in the log files.
Event Type	The type of administrator activity (such as, administrator login, view records, and update user and organization information) that you performed.
Status	The status of the action taken: ■ **Success**: If the action was completed successfully. ■ **Failure**: If the administrator failed to complete the action.
Reason	The reason why the operation failed.
User ID	If the transaction involved modification of user attributes, then this field specifies the name of the user whose attributes were updated or modified.
Target Organization	The organization to which the user belongs.

Report Field	Description
Component	The resource that was used to perform the task. The column values are: ■ Administration Console (Admin Console) ■ RiskFort (RiskFortResourcePack)
Session ID	The unique numerical identifier created each time you log in to Administration Console. This session lasts until you log out.
Instance ID	In case there are multiple instances of RiskMinder Server are running, then this field uniquely identifies the instance that you logged in to. **Note:** This data is used by CA Support personnel to diagnose problems.

RiskMinder Reports

All the RiskMinder configuration-related reports available in the system include:

- Instance Management Report (see page 357)
- Analyze Transactions Report (see page 358)
- Risk Evaluation Detail Activity Report (see page 369)
- Risk Advice Summary Report (see page 372)
- Fraud Statistics Report (see page 373)
- Rule Effectiveness Report (see page 374)
- False Positives Report (see page 374)
- Device Summary Report (see page 375)
- Exception User Report (see page 376)
- Rule Configurations Report (see page 376)
- Rules Data Report (see page 377)

Instance Management Report

This report is available only to the MA. This report displays the details of the Instance Management activities for any or all of the following events:

- System Cache Refresh
- Update Instance Configuration
- Start Up
- Cache Refresh
- Shut Down

The following table lists the information included in an Instance Management Report.

Fields	Description
Instance Name	The name of RiskMinder Server or Case Management Queuing Server instance.
Server Type	The server type (RiskMinder Server or Case Management Queuing Server) on which the activity was performed.
Activity Type	The type of activity performed.
Activity Time	The time the activity was performed.
Instance Configuration	Used for troubleshooting purposes by CA Arcort Support personnel.
Organizations Refreshed	The organizations whose cache was refreshed.

Analyzing Transactions

Important! Only GAs, OAs, and Fraud Analysts (FAs) can analyze the user transactions for the organizations that are in their scope. The MA, UAs, and CSRs *cannot* perform this task.

Viewing the Analyze Transactions report is a multi-step process that can involve:

- Step 1: Viewing Transactions Summary (see page 359)
- Step 2: Viewing Case Details (see page 362)
- Step 3: Viewing Similar Transactions (see page 368)
- Step 4: Marking Transactions for Further Investigation (see page 369)

While looking at all the transactions based on the criteria that you specified in the Transactions Summary page, if you locate one or more suspect transactions, then you can further look into the details of these transactions (Step 2: Viewing Case Details (see page 362)). You can further locate a pattern by viewing similar transactions (Step 3: Viewing Similar Transactions (see page 368)). After you have analyzed the details and discovered patterns, you can mark suspect transactions for further investigation by the CSRs (Step 4: Marking Transactions for Further Investigation (see page 369).)

Step 1: Viewing Transactions Summary

To view the Transactions Summary, perform the following steps:

1. Ensure that you are logged in with proper credentials.
2. Activate the **Reports** tab in the main menu.
3. Click the **RiskFort Reports** submenu.

   The corresponding links for the report type appear in the left-handle task panel.
4. Click the **Analyze Transactions Report** link.
5. From the **Select Organization** list, select the organization whose data you want to filter in the report.

   The Select Transactions page appears.
6. From the **Select Channel** drop-down list, select the channel for which you want to view the transactions.
7. **Enter User Identification** for the user whose transactions you want to view.

   You can search based on either the user name or the account type. If you do not have any accounts configured for the organization, you will be prompted to enter the user name.

   Note: If you do not specify any user details, then all the transactions for the specified **Organization** are displayed.
8. To filter the transactions based on one of following criteria:

   - Select the pre-defined date range based on which you want to filter the transaction data in the **Transaction Date From** and **To** fields.

   or

   - Select the **Last Transactions** option and then select the time interval (in minutes) for which you want to see the latest transactions that were performed.
9. From the **Risk Advice** list, select the advices based on which you would like to filter the data.
10. From the **Secondary Authentication Status** list, select the statuses based on which you would like to filter the data.
11. From the **Fraud Status** list, select the statuses based on which you would like to filter the data.
12. From the **Rule** list, select the rule based on which you would like to filter the transaction data.

    Note: If you want to see the transactions for all rules that matched, then ensure that the default **All Rules** option is selected.

13. **(Only for 3D Secure)** Enter the merchant name in the **Merchant** field, and select the criteria (**Exact**, **Starts with**, **Ends with**, **Contains**) based on which you want to filter the transaction data.
14. Enter the **Device ID** of the device for which you would like to filter the transaction data.
15. Select **Decrypt Sensitive Information** if you want to display the data in clear text.
16. Click **Submit** to generate the Transactions Summary page.

    You can export the information directly to a CSV file by clicking the **Export** button.

    Note: You can view transactions specific to a channel by clicking the **Default** or **3D Secure** tabs.

    The following table describes the fields listed in the Transactions Summary page.

Fields	Description
Details	Click the **detail** link to look into the details of the transaction.
User Name	The name of the user performing the transaction.
Fraud Status	The fraud status of the case. This field can have one of the following statuses: ■ Assumed Fraud ■ Assumed Genuine ■ Confirmed Fraud ■ Confirmed Genuine ■ Undetermined
Country	Based on the IP Address, the country from which the transaction was performed.
IP Address	The IP address of the system or device used for the purchase transaction.
Matched Rule	The rule that matched and for which RiskMinder flagged the transaction as risky.
Transaction Date	The timestamp when the transaction was performed.
Risk Score	The overall risk score returned by RiskMinder for the corresponding transaction. This is a value between 0 and 100.
Risk Advice	The action suggested by RiskMinder after evaluating the Risk Score of the transaction. The possible actions are: ■ ALLOW ■ ALERT ■ DENY ■ INCREASE AUTHENTICATION

Fields	Description
Device ID	The ID of the device used for the transaction.
Model Score	The risk score returned by the Model for the transaction. This is a value between 0 and 100.
Secondary Auth Status	If the Risk Advice is **INCREASE AUTHENTICATION**, then this column specifies the result of the additional authentication that your application returned as feedback to RiskMinder.
Account Type	The account type associated with the transaction. This column is displayed only if you have configured account types for the organization.
Rule Results	The result of all the rules for the transaction. The result is **Y** or **N**.
Account ID	If there is an account ID associated with the user, then this column specifies the account ID that was used to perform the transaction.
Device Type	The type of device involved in the transaction.
Transaction ID	The unique ID generated for each user transaction.
OS	The operating system on the device that was used to perform the transaction.
Browser	The browser that was used to perform the transaction.
Device ID Status	The status of the Device ID: ■ **READ**: The Device ID was read from the device. ■ **NEW**: The Device ID was assigned to the device. ■ **REVERSE LOOKUP**: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.
Action	The type of transaction performed by the user, which can be: ■ Login ■ Wire Transfer ■ Any other value that you specify through your application

Step 2: Viewing Case Details

The Transactions Summary page can also be used to view details of any specific transaction or case. To view details of a specific case:

1. In the Transactions Summary page, click the required **detail** link in the corresponding **Details** column.

   The transaction details are displayed on the page. This page lists the details of the selected transaction, and also allows you to further filter transactions on the basis of available parameters.

   The following table describes the fields listed in the Transaction Details page.

Fields	Description
Basic Transaction Details	
Transaction ID	The unique identifier of the transaction.
Transaction Date	The timestamp when the transaction was performed.
Action	The type of transaction performed by the user, which can be: ■ Login ■ Wire Transfer ■ Any other value that you specify through your application
User Name	The name of the user who performed the transaction.
Fraud Status	The current status of the fraud. Possible values are: ■ Undetermined ■ Assumed Fraud ■ Assumed Genuine ■ Confirmed Fraud ■ Confirmed Genuine
Device ID	The ID of the device used for the transaction.

Fields	Description
Risk Advice	An action suggested by the Risk Assessment module after evaluating the risk score of the selected transaction. The possible actions are: ■ ALLOW ■ ALERT ■ DENY ■ INCREASEAUTH
Matched Rule	The rule that matched and for which RiskMinder flagged the transaction as risky.
Secondary Auth Status	If the Risk Advice is **INCREASE AUTHENTICATION**, then this column specifies the result of the additional authentication that your application returned as feedback to RiskMinder. The possible values are Success and Failure.
Account Type	The account type associated with the transaction.
Account ID	The account ID of the user who performed the transaction.
Model Score	The risk score returned by the Model for the transaction.
Risk Score	The overall risk score returned by RiskMinder for the corresponding transaction. This is a value from 0 through 100.
Location Details	
IP Address	The IP address of the system or device used for the purchase transaction.
City	The city where the transaction was performed by the user.
State	The state to which the user belongs.
Country	The country to which the user belongs.

Fields	Description
Connection Type	The connection type between the user's device and their Internet Service Provider. The possible values are: ■ Satellite ■ OCX ■ Frame Relay ■ TX ■ Dialup ■ Cable ■ DSL ■ ISDN ■ Fixed Wireless ■ Mobile Wireless
Line Speed	The speed of the user's internet connection. This is based on the Connection Type.
IP Routing Type	The IP routing method used for the connection. The possible values are: ■ Fixed: Cable, DSL, OCX ■ AOL: AOL users ■ POP: Dial up to regional ISP ■ Super POP: Dial up to multi-state ISP ■ Cache Proxy: Accelerator proxy, content distribution service ■ Regional Proxy: Proxy for multiple states in a country ■ Anonymizer: Anonymizing proxy ■ Satellite: Consumer satellite or backbone satellite ISP ■ International Proxy: Proxy funneling international traffic ■ Mobile Gateway: Mobile device gateway to Internet ■ Unknown: Cannot currently be determined

Fields	Description
Anonymizer Type	The type of anonymizer, if any, used for the connection. The possible values are: ■ **Private:** Anonymous proxies that are not publicly accessible. These type of anonymizers typically belong to commercial ventures. ■ **Active**: Anonymous proxies that tested positive within the last six months. ■ **Suspect**: Anonymous proxies that tested positive within the last two years, but not the last six months. ■ **Inactive**: Anonymous proxies that did not test positive in the last two years. ■ **Unknown**: Anonymous proxies for which no positive test results are currently available.
Risk Assessment Details	
MFP Match %	The match percentage of the incoming Machine FingerPrint (MFP) with the value stored in the RiskMinder database. This is a numeric value.
Unknown User	Whether the Unknown User rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
Exception User Check	Whether the Exception User Check rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
Negative Country Check	Whether the Negative Country Check rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.

Fields	Description
Device MFP Not Match	Whether the Device MFP Not Match rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
Trusted IP/Aggregator Check	Whether the Trusted IP/Aggregator Check rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
Untrusted IP Check	Whether the Untrusted IP Check rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
User Velocity Check	Whether the User Velocity Check rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
Unknown DeviceID	Whether the Unknown DeviceID rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
Device Velocity Check	Whether the Device Velocity Check rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.

Fields	Description
Zone Hopping Check	Whether the Zone Hopping Check rule matched. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
User Not Associated with DeviceID	Whether the User-Device Association was found in the RiskMinder database. The possible values are: ■ **Yes:** If the rule matched. ■ **No:** If the rule did not match. ■ **N/A:** If the information was not available during risk evaluation.
Device Details	
Device Type	Type of device involved in the transaction.
OS	The operating system on the device that was used to perform the transaction.
Browser	The browser that was used to perform the transaction.
Device ID Status	The status of the Device ID: ■ READ: The Device ID was read from the device. ■ NEW: The Device ID was assigned to the device. ■ REVERSE LOOKUP: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.

Step 3: Viewing Similar Transactions

The small table at the end of the transaction details enables you to specify filter criteria to extract fine-grained data for similar transactions from the RiskMinder database.

Transactions can be further filtered on the basis of the following parameters:

- **Same User Name**: By selecting this option, you can extract all transactions that belong to the same user whose data you are currently viewing.
- **Same Device ID**: By selecting this option, you can extract all transactions done by using the same device that is used for the current transaction details that you are viewing.
- **Same IP Address**: By selecting this option, you can extract all transactions that have the same IP address as the current transaction details that you are viewing.
- **Transaction Date**: By specifying a date range (using the **From** and **To** fields), you can further filter all transactions that were performed in the specified time period.

  or

- **Last Transactions:** By selecting the required time interval (in minutes), you can further filter all the latest transactions that were performed in the specified interval.

Viewing Related Transactions

To view the related transactions:

1. In the Transaction Details page, select any or all of the following options:
   - Same User Name
   - Same Device ID
   - Same IP Address
2. Either:
   a. Enter a date range in the **Transaction Date From** and **To** fields.

   or

   b. Select the **Last Transactions** option and then select latest time interval for which you want to see the related transactions.
3. Click **Show**.

   The Transactions Summary page appears, displaying the records that matched the criteria.

Step 4: Marking Transactions for Further Investigation

After you have analyzed the details of suspect transactions or discovered patterns, you can mark suspect transactions for further investigation by the CSRs. To do so:

1. Ensure that you are logged in with the required privileges.
2. Display the Transactions Summary page, as discussed in "Step 1: Viewing Transactions Summary" (see page 359).
3. Review the transactions that are displayed based on the criteria that you specified.

   See "Step 2: Viewing Case Details" (see page 362).
4. If you want to display similar patterns, follow the steps in "Step 3: Viewing Similar Transactions" (see page 368).
5. Scroll back to the Transactions Summary table.
6. Select the transactions that you suspect by selecting the check boxes corresponding to the transaction in the table.
7. Click the **Mark for Investigation** button to generate cases for the transactions you marked.

   These cases will now appear in the case lists for the CSRs to work on.

Risk Evaluation Detail Activity Report

This report displays *all* transactions performed by RiskMinder Server.

To generate this report, you must specify:

- The **Organization Name**.
- The **Channel.**
- The **User Identification**, if required.

  This can be based on either the user name or account type.
- The **Date Range**.

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

Fields	Description
Date Logged	The timestamp when risk evaluation was performed for the user.
User Name	The unique ID of the user who performed the risk-evaluation activity.
Organization Name	The organization to which the user belongs.

Fields	Description
Transaction Type	The type of risk-evaluation activity that was performed by RiskMinder Server. These activities include: ■ Evaluate Risk ■ Update Attributes ■ Create Associations ■ Delete Associations
Status	The status of the event action taken and can be: ■ **Success**: RiskMinder was able to perform the risk evaluation activity successfully. ■ **Failure**: RiskMinder was not able to perform the risk evaluation activity successfully.
Score	The score generated for the given transaction.
Advice ID	The advice generated by RiskMinder, depending on the score generated. The advice can be one of the following: ■ Allow ■ Deny ■ Alert ■ Increase Authentication
Matched Rule	The rule that matched.
Secondary Authentication Result	The result of secondary authentication that was returned to RiskMinder by your application, if the **Risk Advice** generated by RiskMinder was "Increase Authentication".
Transaction Status	The status of the transaction.
Configuration Name	The ruleset configured for the organization to which the user belongs.
Action	The corresponding action (for example, Login) that was performed for the current Event.
Caller ID	A unique identifier passed to the RiskMinder APIs by your calling application. **Note:** Caller ID can be blank, if your calling application does not set the value.
Transaction ID	The unique numerical identifier created each time you submit a transaction (such as, administrator login, view records, and update user and organization information) to RiskMinder Server. **Note:** You can use this ID to isolate information about a specific transaction in the log files.

Fields	Description
Session ID	The unique numerical identifier created each time you log in to Administration Console. This session lasts until you log out.
Instance ID	If there are multiple instances of RiskMinder Server are running, then this field uniquely identifies the instance that you logged in to. **Note:** This data is used by CA Support personnel to diagnose problems.
Country	The country where the transaction originated. **Note:** This is derived from the **Client IP Address** value.
Client IP Address	The IP address of the end user's system.
Incoming DeviceID	The incoming DeviceID string.
Outgoing DeviceID	The corresponding Device ID that was generated during the transaction, if this is the first transaction from the end user's system.
Device Type	The type of device involved in the transaction.
Device ID Status	The status of the Device ID: ■ READ: The Device ID was read from the device. ■ NEW: The Device ID was assigned to the device. ■ REVERSE LOOKUP: The Device ID was determined by matching the input device signature against the device signatures that were successfully associated with the user.
All Rules Result	The result of all rules applied. If a rule was applied, then the result (**Yes** or **No**) indicates whether the rule returned a match or not.
Account Type	The account type configured for the organization.
Account ID	The account ID of the user who performed the risk-evaluation activity.

Risk Advice Summary Report

The Advice Summary Report provides an overall summary of advices that were returned by RiskMinder over the specified period of time. It also displays a separate table with the detailed summary of all the secondary authentication results.

Note: RiskMinder returns a risk advice for every transaction attempted by the user. Depending on the advice sent by RiskMinder, your application may allow the user to complete a transaction or deny the transaction.

To generate this report, you must specify:

- The **Date Range**.
- The **Channel**
- The **Organization Name**, if required.

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

Fields	Description
Channel	The channel on which the transaction was performed.
Allow	The total number of transactions for which RiskMinder generated the **Allow** advice.
Increase Authentication	The total number of transactions for which RiskMinder generated the **Increase Authentication** advice, and your application prompted the user for an additional authentication.
Alert	The total number of transactions for which RiskMinder generated the **Alert** advice.
Deny	The total number of transactions for which RiskMinder generated the **Deny** advice.
Total	The total number of risk advices generated.

The following table lists the information included in a Secondary Authentication Results Summary Report:

Fields	Description
Channel	The channel on which the transaction was performed.
Success	The total number of all secondary authentication attempts that were successful.
Failure	The total number of all failed secondary authentication attempts by the user.

Fields	Description
Undetermined	The total number of all instances when the result of the secondary authentication was not forwarded by your application to RiskMinder.
Total	The total number of secondary authentications performed, irrespective of the result generated.

Fraud Statistics Report

As explained in the following table, the Fraud Statics report displays statistics for each Risk Advice generated by RiskMinder in the specified time period. Along with the Rule Effectiveness Report and the False Positives Report, this report helps the Fraud Analysts track the performance of their rule set as a function of time.

Parameter	Description
Risk Advice	Specifies the action suggested by RiskMinder after evaluating the risk of each transaction. The generated risk advice can be one of the following: ■ Alert ■ Increase Authentication ■ Allow ■ Secondary Channel ■ Deny
Fraud	Specifies the total number and percentage of all transactions that were reported by RiskMinder as fraudulent.
Genuine	Specifies the total number and percentage of all transactions that were considered genuine by RiskMinder.
Undetermined	Specifies the total number and percentage of all transactions for which RiskMinder did not have sufficient data to generate a risk advice.
Total	Specifies the total for all transactions for each "Risk Advice". It also specifies the overall **Total**.

Rule Effectiveness Report

Rule efficacy changes, and generally degrades with time. Fraudsters find new avenues of attack that circumvent the rules. The business evolves, opening new paths of access or commerce previously unprotected. System changes modify the meaning of data creating subtle downstream effects. For all these reasons, Fraud Analysts find that a major part of their job is the monitoring of the existing rule set. They can use this report to assess the effectiveness of the configured rules and their scores.

The Rule Effectiveness Report tabulates which rules established the outcome for the risk evaluation, as explained in the following table.

Parameter	Description
Rule Name	Lists the rules currently configured in the system.
Advice	Specifies the action suggested by RiskMinder after evaluating the risk of each transaction. The generated risk advice can be one of the following: ■ Increase Authentication ■ Alert ■ Deny
Yesterday Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the last 24 hours of the report generation.
Last 7 Days Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the last 7 days of report generation.
Last 7 Days Daily Average	Specifies the average number of times the corresponding Rule Name was triggered in the last 7 days of report generation.
Last 30 Days Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the last 30 days of report generation.
Last 30 Days Daily Average	Specifies the average number of times the corresponding Rule Name was triggered in the last 30 days of report generation.

False Positives Report

The False Positives Report tabulates which rules established the outcome for the risk evaluation, as explained in the following table.

Parameter	Description
Rule Name	Lists the rules currently configured in the system.

Parameter	Description
Advice	Specifies the action suggested by RiskMinder after evaluating the risk of each transaction. The generated risk advice can be one of the following: ■ Increase Authentication ■ Alert ■ Deny
Transaction Count	Specifies the total number of times the corresponding Rule Name was triggered in the specified time period.
Fraud	Specifies the total number of all transactions for which the corresponding Rule Name generated a false positive result on fraudulent transactions.
Genuine	Specifies the total number of all transactions for which the corresponding Rule Name generated a false positive result on genuine transactions.
Undetermined	Specifies the total number of all transactions for which the corresponding Rule Name did not have sufficient data to generate a risk advice.

Device Summary Report

This report displays the total number of transactions by device type and method of device ID determination.

To generate this report, you must specify:

- The required **Organization Name**.
- The **Channel**.
- The **Date Range**.

The following table lists the information included in a Device Summary Report.

Fields	Description
Device Type	The type of device from which the transaction originated.
DeviceID Read	Number of transactions where the Device ID was read from the device involved in the transaction.
New Device	Number of transactions where the Device ID was assigned to the device involved in the transaction.
Reverse Lookup	Number of transactions where the Device ID was recovered using the Reverse Lookup mechanism.

Fields	Description
Total	Total number of transactions generated from a specific Device Type.

Exception User Report

This report displays the list of all Exception users configured in the RiskMinder system.

To generate this report, you must specify:

- The **Date Range**.
- The required **Organization Name**.
- The **User Name**.

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

Fields	Description
Start Date	The date and time from which the user is considered an exception user in the system.
End Date	The date and time when the user stops being an Exception User in the system.
User	The unique user name.
Reason	The reason for making the user an Exception User in the system.
Organization	The organization to which the administrator belongs.

Rule Configurations Report

The Rule Configurations Report displays the overall summary of all the rules deployed for an organization. To generate this report, you must specify:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Status** of the target information.

The following table lists the information included in a Rule Configurations Report.

Fields	Description
Rule Name	The name of the rule.
Enabled	Indicates whether the rule is enabled or not.

Fields	Description
Priority	The priority of the rule.
Score	The score generated for the given transaction.
Advice	The advice generated by RiskMinder, depending on the score generated. The advice can be one of the following: ■ Allow ■ Deny ■ Alert ■ Increase Authentication
Rule Expression	The rule expression that is evaluated.
Channels	The channel for which the rule is deployed.
Actions	The actions that are permissible for the rule.
Rule Mnemonic	The short name of the rule.
Description	The description of the rule.

Rules Data Report

The Rules Data Report displays the summarized data for the selected list that has been uploaded for an organization. (See Uploading Rule List Data (see page 202) for detailed information on list data and how to upload a list to be used by a rule.)

To generate this report, you must specify:

- The required **Organization Name**.
- The required **Ruleset Name**.
- The **Rulelist Type.**
- The uploaded **List** name.
- The **Status** of the target information.

Case Management Reports

See "Generating Case Management Reports" (see page 342) for detailed information on the reports available in this category.

Generating Reports

This section covers:

- Notes for Generating Reports (see page 378)
- Generating Reports (see page 379)

Notes for Generating Reports

While generating reports, remember that:

- The administrator can *only* generate the reports of the organizations on which they have the scope.
- The administrator can generate the report of their subordinate or peers.

  For example, an Organization Administrator (OA) can generate the reports of an OA and User Administrator (UA).
- If you are using Oracle database, then ensure that you have enabled the UNLIMITED TABLESPACE privilege.

Generating Reports

To generate any of the administrator- or RiskMinder-specific reports:

1. Ensure that you are logged in with proper credentials (MA, GA, OA, or UA.)
2. Activate the **Reports** tab in the main menu.
3. If you want to generate:
   - Administrator activity report, then click the **Administrator Reports** submenu.
   - RiskMinder-specific report, then click the **RiskFort Reports** submenu.

   The corresponding links for the report type appear in the left-handle task panel.
4. Based on the report you want to generate, click the required link from the left-hand submenu.

   Note: RiskMinder allows you to choose to display either clear text data or encrypted data in Administrator Reports. For all Administrator Reports, select **Decrypt Sensitive Information** if you want to display the data in clear text in the report.
5. Specify one or more of the following criteria, as applicable, to view the report:
   - The **Date Range** from the drop-down list.

     or
   - A pre-defined date range in the **From** and **To** fields.
6. Depending on the report, additionally you might have to specify the following:
   - **Organization Name** for the required organizations whose data you want to include in the report.
   - **User Name** (or **Administrator Name**), based on the report you want to generate:
     - Enter a user name (for User Activity reports.)

     or
     - Enter the administrator name (for Administrator Activity reports.)
   - **Ruleset Name** for the required ruleset whose data you want to include in the report.
7. Click **Display Report** to generate the report based on the criteria you specified.

Exporting Reports

Administration Console provides the ability to export reports to a file. By exporting a report, you can save a local copy of the report, which enables you to track trends. You can also work with the saved report data in another application.

The exported reports are generated in the comma-separated value (CSV) format that can be viewed by using text editors and spreadsheet applications, such as Microsoft Excel. The export option is available through the **Export** button, which appears at the top-right of every rendered report.

To export a report to a local file:

1. Generate the required report. See "Generating Reports" (see page 379) for detailed instructions to do so. The report opens.
2. Click **Export**.

   You are prompted to save or open the report.
3. Click **Open** (**with**) or **Save** (**file**). If you choose to save the report, then you must specify the download location.

   This file can later be viewed by using the appropriate application.

arreporttool: Report Download Tool

The arreporttool enables you to export reports in the comma-separated value (CSV) format from the command line. You can then view these reports by using text editors and spreadsheet applications, such as Microsoft Excel.

Using the Tool

The arreporttool.jar file is available at the following location:

On Windows:

`<install_location>\Arcot Systems\tools\common\arreporttool`

On UNIX Platforms:

`<install_location>/arcot/tools/common/arreporttool`

Syntax:

Run the following command to see the help associated with the tool:

```
java -jar arreporttool.jar --help
```

Run the following command to use the tool:

```
java -jar arreporttool.jar –-protocol <protocol> --host <host>
--port CA Portal --admin-orgid <admin-organization>
--admin-id <admin-user-id> --admin-password <password>
[--report-type hour | day | month [duration] | range]
--report-id <Report ID> --reporturl <Url of the report>
--is-filter-req <true | false> --data-type <Data Type>
--reportdata [Report Data] --start-date-time <date-and-time> [--end-date-time
<date-andtime>] [--logfile <logfile>]
[--log-level <loglevel>][log-file-max-size] <logfilesize>] [--organizations <target
orgNames>] [--userName <User/Admin Name>] [--output-file <output-file>.CSV]
[--is-url-encoded [true|false]]
```

The following table describes the options supported by the tool.

Option	Description
protocol	The protocol that is used for communication. The possible values are http and https.The default protocol is http.
host	The host name or the IP address of the system where you have deployed Administration Console.
port	The port at which the Console is listening.
admin-orgid	The organization to which the administrator belongs.
admin-id	The unique administrator ID.
admin-password	The administrator password.

Option	Description
report-type	Specify hour, day, month, or range. ■ Hour, day, month can be followed by a numeric number. For example, --report-type day 2 indicates two days of records from the start-date-time is specified. ■ Range: If range is specified, end-date-time is mandatory.
report-id	Identifier of the report to be fetched. See "List of Report Identifiers" (see page 383) for the list of report identifiers that you can use.
reporturl	Administrator URL of the report. See "List of Report URLs" (see page 383) for the list of report URLs that you can use.
is-filter-req	This is true by default. Set this value to false for reports that do not have a filter page, for example, RiskFort reports.
data-type	This is applicable only for RiskFort reports. This option specifies whether data type is ACTIVE or STAGING.
reportdata	In addition to start and end dates, certain reports need additional filters. These additional filters can be specified as report data. The report data must be in the 'key=value' format. You can use a semicolon to separate multiple key-value pairs. The report data must be URL-encoded if it contains ; or =. Ensure that you set the is-url-encoded parameter to true if an URL-encoded value is passed.
start-date-time	Specify the data or time after which report content must be fetched. **Format**: MM/dd/yyyy HH:mm:ss Hour (HH) and Minutes (mm) are optional and are used only for hourly reports. For daily and monthly reports, only the date part is used. **Example**: 03/21/2010 09:10:20
end-date-time	[Optional] Specify the end date and time till which report content should be selected.
logfile	[Optional] Specify the location of the log file. If no log file is specified, the file is automatically created in the current directory.
log-level	[Optional] Specify the log level. Default log level is INFO.
log-file-max-size	[Optional] Specify the maximum size of the log file. The default value is 10 MB.

Option	Description
organizations	[Optional] Specify semicolon-separated target organization names for the report. You *must* specify this value for reports that have organizations as a mandatory parameter. The value must be URL-encoded if the organization name contains a semicolon(;). Ensure that you set the is-url-encoded parameter to true if a URL-encoded value is passed.
userName	[Optional] Specify the user or administrator name.
output-file	[Optional] Specify the output file where the report content must be written. **<reporttype>-timestamp.CSV** is used.
is-url-encoded	[Optional] Set this value to true or false depending on whether your report data and organizations contain URL-encoded information. The default value is false.

List of Report Identifiers

The following table lists the report identifiers that you can use for the report-id argument.

Report	Report ID
My Activity Report	AAC.ViewMyActivityReport
Administrator Activity Report	AAC.ViewActivityReport
User Activity Report	AAC.ViewUserActivityReport
Organization Report	AAC.ViewOrgActivityReport
User Creation Report	AAC.ViewUserCreationReport

List of Report URLs

The following table lists the report URLs that you can use for the reporturl argument.

Report	Report URL
My Activity Report	/Ac_AdminMyActivity/view.htm
Administrator Activity Report	/Ac_Adminreport/view.htm
User Activity Report	/Ac_AdminUserActivity/view.htm
Organization Report	/Ac_AdminOrgActivity/view.htm
User Creation Report	/Ac_AdminUserCreation/view.htm

Examples of Using the Tool

To download the User Activity Report:

```
java –jar arreporttool.jar --protocol http --host localhost --port 8080  arcot
--admin-id ga --admin-password ga123 --report-id AAC.ViewUserActivityReport
--report-url /Ac_AdminUserActivity/view.htm --startdate-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log ARCOT –-userName ua
```

To download the Organization Report:

```
java -jar arreporttool.jar --protocol http --host localhost --port 8080  arcot
--admin-id ga --admin-password ga123 --report-id AAC.ViewOrgActivityReport
–report-url /Ac_AdminOrgActivity/view.htm --start-date-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log --organizations ARCOT;TEST
```

Appendix A: RiskMinder Rule Tags

Rules take data elements, called *Tags*, as input. For example, two common data elements are the end user's country and the transaction amount. This data is provided in the evaluateRisk()API call through extensible data structures called *contexts*. For more information, see the *CA RiskMinder Java Developer's Guide*.

This appendix describes the tags that you can use in your rules.

Data elements are referenced in RiskMinder rules either using an explicit reference called a *TagName*, or implicit reference by the context of the rule. You can use the data listed in the following table to include in your rules. Some of this data is provided in the RiskMinder evaluateRisk() API call and other data is derived through lookup, such as the geolocation of the end user's or cardholder's IP address.

The data in the following table is classified into the following categories:

- **User**: Provides information about the user and the account.
- **Device**: Provides information about the device used to originate the transaction.
- **General Transaction**: Provides information about elements of every transaction, such as the channel and action.
- **Currency**: Provides information such as currency conversion rate and base currency.
- **Location**: These elements are derived from a maintained database of IP geolocation, which provides location data and connection attributes of the IP address.
- **Internal Parameters:** Support the construction of custom rule types.

Tag Name	Description
User Information	
IDENTITY.USERID	The encrypted version of the user identifier.
RULESET.GROUPNAME	The organization name.
Device Information	
DEVICEID.http	The alpha-numeric ID assigned by RiskMinder for this device.
DEVICEID.flash	The Flash device ID string specific to the transaction.
DEVICESIG	The device signature.
SHORTDEVICESIG	The compact form of the device signature.
AGGREGATORINFO	Aggregator ID string specific to the transaction.

Tag Name	Description
RULE.SIGPASSTHRESHOLD	Pass threshold used by the Device MFP Not Match rule.
General Transaction Information	
RULESET.CHANNELNAME	The channel using which the user accesses the system.
TRANSACTION.TXNID	The numeric identifier for this transaction generated by RiskMinder.
TRANSACTION.EXT	Name-value Extensible element string sent by the client.
Currency Information	
BASE_CURR_CODE	Numeric designation corresponding to the 3-letter designation of the base currency of the organization.
BASE_CURR_AMOUNT	Transaction amount converted to the Base Currency.
BASE_CONVERSION_RATE	Conversion rate from transaction currency to the base currency of the organization.
Location Information	
RULESET.COUNTRYISO	Contains the two letter ISO 3166 alpha country code of the country, for example AU.
RULESET.STARTIP	Starting IP for the user IP block.
RULESET.ENDIP	Ending IP for the user IP block.
RULESET.GEOLAT	Latitude is expressed as a floating point number with positive numbers representing North and negative numbers representing South.
RULESET.GEOLONG	Longitude is expressed as a floating point number with positive numbers representing East and negative numbers representing West.

Tag Name	Description
RULESET.GEOCF	Confidence Factor (CF) in the geolocation. Confidence Factors are calculated based on the precision, completeness, and consistency of the data available to assign a specific geographic location to an IP address range. Confidence Factors are provided for Country, State, and City. Their value ranges from 1 to 99. A higher value indicates that the likelihood of a correct location assignment is higher; a lower value indicates the opposite. These values are not percentages. Their intended use is as a relative measure of "confidence" on the correctness of the corresponding location assignment.
Internal Parameters	
RULE.USERCONTEXT	User context information used internally by the rules engine to store state information.
RULE.DEVICECONTEXT	Device context information used internally by the rules engine to store state information.
ADDONRULE.DESCRRESULT	The concatenated string of results from the add-on rules called till this point.
ADDONRULE.ANNOTATION	The concatenated strings of annotations set by all add-on rules called till this point.
RULE.PARAMETERS	Name-Value parameters configured for the rule.
RULE.RULEMNEMONIC	Rule mnemonic configured for the rule.

Appendix B: RiskMinder Logging

To effectively manage the communication between RiskMinder Server and your application, it is necessary to get information about the activity and performance of the Server and other components, as well as any problems that might have occurred.

This appendix describes the log files supported by RiskMinder, the severity levels that you will see in these files, and the formats of these log files. It covers the following topics:

- About the Log Files (see page 390)
- Format of RiskMinder Server and Case Management Server Log Files (see page 398)
- Format of the UDS and Administration Console Log Files (see page 399)
- Supported Severity Levels (see page 399)

About the Log Files

The RiskMinder log files can be categorized as:

- Installation Log File (see page 391)
- Startup Log Files (see page 391)
- Transaction Log Files (see page 394)
- Administration Console Log File (see page 396)
- UDS Log File (see page 397)

The parameters that control logging in these files can be configured either by using the relevant INI files (as is the case with the UDS and Administration Console log files) or by using Administration Console itself (as is the case with the RiskMinder and Case Management Queuing Server log file.) The typical logging configuration options that you can change in these files include:

- **Specifying the log file name and path:** RiskMinder enables you to specify the directory for writing the log files and storing the backup log files. Specifying the diagnostic logging directory allows administrators to manage system and network resources.
- **Specifying the log file size:** You can specify the maximum number of bytes that the log file can contain. When the log files reach this size, a new file with the specified name is created and the old file is moved to the backup directory.
- **Using log file archiving:** As RiskMinder components run and generate diagnostic messages, the size of the log files increases. If you allow the log files to keep increasing in size, then the administrator must monitor and clean up the log files manually. RiskMinder enables you to specify configuration options that limit how much log file data is collected and saved. RiskMinder allows you to specify the configuration option to control the size of diagnostic logging files. This helps you determine a maximum size for the log files. When the maximum size is reached, older log information is moved to the backup file before the newer log information is saved.
- **Setting logging levels:** RiskMinder also allows you to configure logging levels. By configuring logging levels, the number of messages saved to diagnostic log files can be reduced. For example, you can set the logging level so that the system only reports and saves critical messages. See "Supported Severity Levels" (see page 399) for more information on the supported log levels.
- **Specifying time zone information:** RiskMinder enables you to use either the local time zone or GMT for time stamping the logged information.

Installation Log File

When you install RiskMinder, the installer records in the Arcot_RiskFort_Install<*timestamp*>.log file all the information that you provide during the installation and the actions that it performs, such as creating the Arcot directory structure and making registry entries. The information in this file is very useful in identifying the source of problems if the RiskMinder installation did not complete successfully.

The default location of this file is:

Windows:

<*install_location*>\<*log_file_name*>

UNIX-Based:

<*install_location*>/<*log_file_name*>

Startup Log Files

Because RiskMinder comprises two server modules, RiskMinder Server and Case Management Queuing Server, you will see two startup log files:

- RiskMinder Server Startup Log File (see page 391)
- Case Management Queuing Server Startup Log File (see page 393)

The default location of these files is:

Windows:

<*install_location*>\Arcot Systems\logs\

UNIX-Based:

<*install_location*>/arcot/logs/

RiskMinder Server Startup Log File

When you start RiskMinder Server, it records all startup (or boot) actions in the arcotriskfortstartup.log file. The information in this file is very useful in identifying the source of problems if the RiskMinder service does not start up.

In this file, all logging-related parameters specified under the [arcot/riskfort/logger] section are controlled by Administration Console. To configure these logging parameters, you must use the instance-specific configuration page that you can access by clicking the required instance in the **Instance Management** page.

Changing RiskMinder Startup Logging Parameters

To change the logging parameters that you see when RiskMinder Server starts up:

1. Navigate to the conf directory in ARCOT_HOME.
2. Open arcotcommon.ini in a text editor of your choice.
3. Add the following section at the end of the file:

```
[arcot/riskfort/startup]
LogDir=logs
LogFileSize=2097152
BackupLogFileDir=logs/backup
LogLevel=2
LogTimeGMT=0
LogTrace=0
```

The following table provides details about these parameters.

Parameter	Default	Description
LogDir	logs	The location of the default log directory. **Note:** This path is relative to ARCOT_HOME (Windows:<*install_location*>\Arcot Systems Linux:<*install_location*>/arcot/).
LogFileSize	10485760	The maximum number of **bytes** the log file can contain. When a log file reaches this size, a new file is created and the old file is moved to the location specified for BackupLogFileDir.
BackupLogFileDir	logs/backup	The location of the directory where backup log files are maintained, after the current file exceeds LogFileSize bytes. **Note:** This path is relative to ARCOT_HOME (Windows:<*install_location*>\Arcot Systems Linux:<*install_location*>/arcot/).
LogLevel	1	The default logging level for the server, unless an override is specified. The possible values are: ■ 0 FATAL ■ 1 WARNING ■ 2 INFO ■ 3 DETAIL

Parameter	Default	Description
LogTimeGMT	0	The parameter that indicates the time zone of the time stamp in the log files. The possible values are: ■ 0 Local Time ■ 1 GMT

1. Set the required values for the parameters that you want to change.
2. Save and close the file.
3. Restart RiskMinder Server.

Case Management Queuing Server Startup Log File

When you start the Case Management Queuing Server, it records all startup (or boot) actions in the arcotriskfortcasemgmtstartup.log file. The information in this file is useful in identifying the source of problems if the Case Management Queuing service does not start up.

In this file, all logging-related parameters (specified under the [arcot/riskfortcasemgmtserver/logger]section) are controlled by Administration Console. To configure these parameters, you must use the instance-specific configuration page that you can access by clicking the required instance in the **Instance Management** page.

Changing Case Management Queuing Server Startup Logging Parameters

To change the logging parameters that you see when Case Management Queuing Server starts up:

1. Navigate to the conf directory in ARCOT_HOME.
2. Open arcotcommon.ini in a text editor of your choice.
3. Add the following section at the end of the file:

   ```
   [arcot/riskfortcasemgmtserver/startup]
   LogDir=logs
   LogFileSize=2097152
   BackupLogFileDir=logs/backup
   LogLevel=2
   LogTimeGMT=0
   LogTrace=0
   ```

   See the table in RiskMinder Server Startup Log File (see page 391) for details of these parameters
4. Set the required values for the parameters that you want to change.
5. Save and close the file.
6. Restart Case Management Queuing Server.

Transaction Log Files

The transaction logs consist of:

- RiskMinder Server Log (see page 395)
- Case Management Server Log File (see page 395)

RiskMinder Server Log

RiskMinder records all requests processed by the server and related actions in the arcotriskfort.log file. The default location of this file is:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

Note: You cannot use the RiskMinder logger to configure your application's logs. You can access these logs by using the tool used by the third-party application server, such as Apache Tomcat or IBM Websphere, which is hosting your application.

All logging-related parameters can be configured by using Administration Console. To do so, you must use the instance-specific configuration page that you can access by clicking the required instance in the **Instance Management** page.

In addition to the log file path, the maximum log file size (in bytes), backup directory, logging level, and timestamp information, you can control whether you want to enable trace logging. See "Format of RiskMinder Server and Case Management Server Log Files" (see page 398) for details of the default format used in the file.

Case Management Server Log File

When you deploy the Case Management Server module and subsequently start it, the details of all its actions and processed requests are recorded in the arcotriskfortcasemgmtserver.log file. The default location of this file is:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

All logging-related parameters (specified under the [arcot/riskfortcasemgmtserver/logger] section) can be configured by using Administration Console. To do so, you must use the instance-specific configuration page that you can access by clicking the required instance in the **Instance Management** page.

In addition to the log file path, the maximum log file size (in bytes), backup directory, logging level, and timestamp information, you can control whether you want to enable trace logging. See "Format of RiskMinder Server and Case Management Server Log Files" (see page 398) for the details of the default format used in the file.

Administration Console Log File

When you deploy Administration Console and subsequently start it, the details of all its actions and processed requests are recorded in the arcotadmin.log file. This information includes:

- Database connectivity information
- Database configuration information
- Instance information and the actions performed by this instance
- UDS configuration information
- Other Administration Console information specified by the Master Administrator, such as cache refresh

The information in this file helps you identify the source of the problems if Administration Console does not start up. The default location of this file is:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

The parameters that control logging in these files can be configured by using the adminserver.ini file, which is available in the conf folder in ARCOT_HOME.

In addition to the logging level, log file name and path, the maximum log file size (in bytes), log file archiving information, you can control the layout of the logging pattern for the Console by specifying the appropriate values for log4j.appender.debuglog.layout.ConversionPattern.

See "Format of the UDS and Administration Console Log Files" (see page 399) for details of the default format used in the file.

UDS Log File

Important! This file is generated only if you deployed the arcotuds.war file to enable LDAP connectivity.

All User Data Service (UDS) information and actions are recorded in the arcotuds.log file. This information includes:

- UDS database connectivity information
- UDS database configuration information
- UDS instance information and the actions performed by this instance

The information in this file is useful in identifying the source of problems if Administration Console could not connect to the UDS instance. The default location of this file is:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

The parameters that control logging in this files can be configured by using the udsserver.ini file, which is available in the conf folder in ARCOT_HOME.

In addition to the logging level, log file name and path, the maximum file size (in bytes), and archiving information, you can control the layout of the logging pattern for UDS by specifying the appropriate values for log4j.appender.debuglog.layout.ConversionPattern.

See "Format of the UDS and Administration Console Log Files" (see page 399) for details of the default format used in the file.

Format of RiskMinder Server and Case Management Server Log Files

The following table describes the format of the entries in the RiskMinder log file, arcotriskfort.log, as discussed in "RiskMinder Server Log" (see page 395).

Column	Description
Time Stamp	The time the entry was logged and translated to the specified time zone. The format of logging this information is: www mmm dd HH:MM:SS.mis yy z In the preceding format: ■ www represents weekday. ■ mis represents milliseconds. ■ z represents the time zone you specified in the arcotcommon.ini file.
Log Level (or Severity)	The severity level of the logged entry. See "Supported Severity Levels" (see page 399) for detailed information.
Process ID (pid)	The ID of the process that logged the entry.
Thread ID (tid)	The ID of the thread that logged the entry.
Transaction ID	The ID of the transaction that logged the entry.
Message	The message logged by the Server in the free-flowing format. **Note:** The granularity of this message depends on the Log Level that you set in arcotcommon.ini.

Format of the UDS and Administration Console Log Files

The following table describes the format of the entries in the following log files:

- arcotuds.log (UDS Log File (see page 397))
- arcotadmin.log (Administration Console Log File (see page 396))

Column	Associated Pattern (In the Log File)	Description
Time Stamp	%d{yyyy-MM-dd hh:mm:ss,SSS z} :	The time when the entry was logged. This entry uses the application server time zone. The format of logging this information is: yyyy-MM-dd hh:mm:ss,mis z Here: ■ mis represents milliseconds. ■ z represents the time zone.
Thread ID	[%t] :	The ID of the thread that logged the entry.
Log Level (or Severity)	%-5p :	The severity level of the logged entry. See "Supported Severity Levels" (see page 399) for more information.
Logger Class	%-5c{3}(%L) :	The name of the logger that made the log request.
Message	%m%n :	The message logged by the Server in the log file in the free-flowing format. **Note:** The granularity of the message depends on the Log Level that you set in the log file.

Refer to the following URL for customizing the PatternLayout parameter in the UDS and Administration Console log files:

http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html

Supported Severity Levels

A *log level* (or *severity level*) enables you to specify the level of detail of the information stored in the RiskMinder logs. This also enables you to control the rate at which the log file will grow.

Server Log File Severity Levels

The following table describes the log levels that you see in server log files, in the *decreasing* order of severity.

Log Level		**Description**
0	FATAL	Use this log level for serious, non-recoverable errors that can cause the abrupt termination of the RiskMinder service. At the FATAL level, only situations which indicate a fatal problem will be logged.
1	WARNING	Use this log level for undesirable run-time exceptions, potentially harmful situations, and recoverable problems that are not yet FATAL.
2	INFO	Use this log level for capturing information on run-time events. In other words, this information highlights the progress of the application, which might include changes in: ■ Server state, such as start, stop, and restart. ■ Server properties. ■ State of services. ■ State of processes on the Server. For example, there are some logs that will always be printed to indicate that requests are being received and that they are being processed. These logs appear at the INFO level.
3	LOW DETAIL	Use this log level for logging detailed information for debugging purposes. This might include process tracing and changes in Server states.

Note: When you specify a log level, messages from all other levels of *higher* significance are reported as well. For example, if the LogLevel is specified as 3, then messages with log levels of FATAL, WARNING, and INFO are also captured.

Administration Console and UDS Log File Severity Levels

The following table describes the log levels that you see in the Administration Console and UDS log files, in the *decreasing* order of severity.

Log Level		**Description**
0	OFF	Use this log level to disable all logging.
1	FATAL	Use this log level for serious, non-recoverable errors that can cause the abrupt termination of the RiskMinder service.

Log Level		**Description**
2	WARNING	Use this log level for undesirable run-time exceptions, potentially harmful situations, and recoverable problems that are not yet FATAL.
3	ERROR	Use this log level for recording error events that might still allow the application to continue running.
4	INFO	Use this log level for capturing information on run-time events. In other words, this information highlights the progress of the application, which might include changes in: ■ Server state, such as start, stop, and restart. ■ Server properties. ■ State of services. ■ State of a processes on the Server.
5	TRACE	Use this log level for capturing finer-grained informational events than DEBUG.
6	DEBUG	Use this log level for logging detailed information for debugging purposes. This might include process tracing and changes in Server states.
7	ALL	Use this log level to enable all logging.

Note: When you specify a log level, messages from all other levels of *higher* significance are reported as well. For example, if the LogLevel is specified as 4, then messages with log levels of FATAL, WARNING, ERROR, and INFO are also captured.

Sample Entries for Each Log Level

The following subsections show a few sample entries (based on the Log Level) in the **RiskMinder log files.**

FATAL

```
May 27 18:31:01.585 2010 GMT FATAL: pid 4756 tid 5152: 0: 0: Cannot continue due to
ARRF_LIB_init failure, SHUTTING DOWN
```

WARNING

```
May 24 14:47:39.756 2010 GMT WARNING: pid 5232 tid 5576: 0: 110000: EVALHTTPCALLOUT
: Transport Exception : create: No Transports Available
```

INFO

```
May 24 14:41:43.758 2010 GMT INFO: pid 3492 tid 4904: 0: 109002: Error in
ArPFExtRuleSetEval::evaluate Could not get user context (two parallel requests)
```

```
May 25 10:01:28.131 2010 GMT WARNING: pid 1048 tid 3104: 8: 0: Error in
ArRFCaseStatus::startInit: No data found
```

DETAIL

```
May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering USERRISKEVALVELOCITY Rule Evaluation function

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE: VELOCITY_DURATION=[60],
VELOCITY_DURATION_UNIT=[MINUTES],                VELOCITY_TRANSACTION_COUNT=[5]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering UserRiskEvalVelocityRule
durationToTimeConvertor

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting
ArUserRiskEvalVelocityDBO::decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting UserRiskEvalVelocityRule
callUserEvalVelocityRule

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.RESULT=[0]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.DETAIL=[RESULT=0;TCOUNT=2;
ACT=mection]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting USERRISKEVALVELOCITY Rule Evaluation function
```

Appendix C: Geolocation and Anonymizer Data

RiskMinder uses geolocation and IP checking in close conjunction to prevent high risk activity. These capabilities use the IP address of end users to:

- Verify that they are not accessing from a country or region that you have blacklisted.
- Verify that they are not moving faster than is actually possible.
- Verify that they are not hiding their location.
- Verify that they are not coming from an IP address that you have blacklisted.

You can decide the mitigating action that you want to choose, which may range from alerting your fraud or security team of possible compromise, automatically requiring additional authentication from the end user, or simply denying access.

This appendix discusses the use of IP geolocation data and Negative IP checks in RiskMinder. Together, these two capabilities provide one of the major components of RiskMinder fraud and high risk access detection. They support the following checks that are provided as part of the RiskMinder out-of-the-box rule settings:

- Geolocation (Negative Country List)
- End user change in access location (Zone hopping)
- Anonymizer data (Negative IP Types)
- Administrator-defined negative IPs (Negative IP Address List)

This appendix covers the following topics:

- Understanding Geolocation and Anonymizer Data (see page 406)
- Using Geolocation Data in RiskMinder Rules (see page 406)
- Using Anonymizer Data (see page 411)
- Using the Negative IP Address List (see page 411)

Understanding Geolocation and Anonymizer Data

Quova Inc., an industry leading provider of geolocation information, provides RiskMinder geolocation and anonymizer data. Quova provides the following types of data to RiskMinder:

- **Geolocation data**. This data classifies each IP by latitude, longitude, continent, country, and city. By default, the data is used in the Negative Country Check rule and in calculating the distance for the Zone Hopping Check rule. You can also use this data for any rules that you create by using the Rule Builder. The Country and City elements are both useful for checks on the point of access.
- **Connection information**. Each IP is classified by routing type, connection type, and line speed. This information, especially routing type, is useful in assessing the validity of the geolocation information. For example, if the connection type is Satellite, then the user's location is not reliable. In practice, you can ignore this information for geolocation purposes. However, fixed connection types such as cable, DSL, and OCX are less likely to be origins of fraud because their locations are more easily backtracked to Internet accounts. You can use this data to evaluate fraud.
- **Anonymizer data**. Quova performs rigorous testing of IP addresses to determine if their location information is reliable. As part of this testing, Quova identifies some IP addresses as "Anonymizers". IP addresses with this status have tested positive as anonymous proxies that are used to hide the true location of the end user. While this does not necessarily indicate that the intent is fraudulent, it does clearly indicate that the user is hiding their location, and therefore represents a high risk access potential.

Using Geolocation Data in RiskMinder Rules

This section describes the following:

- The geolocation information that is used in the following RiskMinder rules:
  - Negative Country Check (see page 407)
  - Zone Hopping Check (see page 407)
- The geolocation data that Quova provides for each routable IP address.
  - IP Routing Type (see page 407)
  - Connection Type (see page 408)
  - Line Speed (see page 409)
  - Region (see page 410)
  - Continent (see page 410)

Negative Country Check

You can use the Manage List Data and Category Mappings page in Administration Console to configure the Negative Country List by adding or removing countries that you consider high risk. Typically, you can define this to be a list of countries where access is always verified using some form of Increased Authentication. However, you can also use this as a Deny rule and list only a small set of countries in the Negative Country List. For financial transactions, you can combine the Negative Country Check rule with an amount-based rule to reduce the number of cases. For general access control, the rule is defined as an Increase Authentication risk advice to trigger a more stringent login process. In these situations, cases are not created.

Zone Hopping Check

The location latitude and longitude are used in the Zone Hopping Check rule. This rule checks the required speed of physical travel required for the user to make successive transactions from the IP addresses they used for access. If the users are traveling too fast, then you must conclude that either two people were accessing the account or the user did something, either intentionally or inadvertently, to mask their true location. CA suggests that you start by setting the values of the Zone Hopping Check rule to the default values provided. Based on performance, you can tune the settings of this rule to meet the requirements of your particular user base. In its default settings, you should expect the rule to fire about 0.02% of the time. The false positive rate for this rule is good at under 10:1.

IP Routing Type

IP Routing Type is an attribute of the IP address that determines the likelihood that the user's location matches the location of the IP address. The following table describes the possible values that you can use for IP Routing Type.

IP Routing Type	Description
fixed	User IP is at the same location as the user.
anonymizer	User IP is located within a network block that has tested positive for anonymizer activity. This means the user is potentially hiding their true location by using a service that deliberately proxies all user traffic.
aol: aol pop aol dialup aol proxy	User is a member of the AOL service; Quova can identify the user country in most cases; any regional info more granular than country is not possible. Please note that in GeoPoint AOL IPs are denoted by a simple Y/N (Yes/No).
pop	User is dialing into a regional ISP and is likely to be near the IP location; the user could be dialing across geographical boundaries.

IP Routing Type	Description
superpop	User is dialing into a multi-state or multi-national ISP and is not likely to be near the IP location; the user could be dialing across geographical boundaries.
satellite	A user connecting to the Internet through a consumer satellite or a user connecting to the Internet with a backbone satellite provider where no information about the terrestrial connection is available. In both cases, the user can be anywhere within the beam pattern of the satellite, which typically spans a continent or more.
cache proxy	User is proxied through either an Internet accelerator or content distribution service; user could be in any location.
international proxy	A proxy that contains traffic from multiple countries.
regional proxy	A proxy (not anonymizer) that contains traffic from multiple states within a single country.
mobile gateway	A gateway to connect mobile devices to the public internet. For example, WAP is a gateway used by mobile phone providers.
unknown	Routing method is not known or is not identifiable in the above descriptions.

Connection Type

Connection Type indicates the data connection between a device or private LAN to the public Internet provider. The following table describes the possible values that you can use for Connection Type.

Connection Type	Description
ocx	This represents OC-3 circuits, OC-48 circuits, etc. which are used primarily by large backbone carriers.
tx	This includes T-3 circuits and T-1 circuits still used by many small and medium companies.
satellite	This represents high-speed or broadband links between a consumer and a geosynchronous or low earth orbiting satellite.
framerelay	Frame relay circuits may range from low to high speed and are used as a backup or alternative to T-1. Most often they are high-speed links, so GeoPoint classifies them as such.
dsl	Digital Subscriber Line broadband circuits, which include aDSL, iDSL, and sDSL. In general, ranges in speed from 256k to 20MB per second.

Connection Type	Description
cable	Cable Modem broadband circuits, offered by cable TV companies. Speeds range from 128k to 36MB per second, and vary with the load placed on a given cable modem switch.
isdn	Integrated Services Digital Network high-speed copper-wire technology, support 128K per second speed, with ISDN modems and switches offering 1MB per second and greater speed.
dialup	This category represents the consumer dialup modem space, which operates at 56k per second. Providers include Earthlink, AOL, and Netzero.
fixed wireless	Represents fixed wireless connections where the location of the receiver is fixed. Category includes WDSL providers, such as Sprint Broadband Direct, as well as emerging WiMax providers.
mobile wireless	Represents cellular network providers such as Cingular, Sprint, and Verizon Wireless who employ CDMA, EDGE, EV-DO technologies. Speeds vary from 19.2k per second to 3MB per second.
unknown	GeoPoint was unable to obtain any connection type or the connection type is not identifiable in the above descriptions.

Line Speed

The speed of the Connection Type (see page 408) between the device or private LAN and the public Internet provider. The following table describes the possible values that you can use for Line Speed for each of the Connection Types.

Line Speed	Corresponding Connection Type
high	OCX, TX, and Framerelay
medium	Satellite, DSL, Cable, Fixed Wireless, and ISDN.
low	Dialup and Mobile Wireless.
unknown	Quova was unable to obtain any line speed information.

Region

For convenience, Quova has divided the U.S. into ten geographical regions:

- Northeast
- Mid Atlantic
- Southeast
- Great Lakes
- Midwest
- South Central\
- Mountain
- Northwest
- Pacific
- Southwest

A complete listing can be found under Reference Data, in the **Download** section of the Quova Extranet. Refer to these text files for the latest information.

Continent

Quova recognizes eight continents:

- Africa
- Antarctica
- Asia
- Australia
- Europe
- North America
- Oceania (Melanesia, Micronesia, Polynesia)
- South America

Using Anonymizer Data

IP addresses can also be classified with an anonymizer status. You can control the types of anonymizer IPs that you include in the rule. The different categories of negative IP types are:

- Negative
- Active
- Suspect
- Private
- Inactive
- Unknown

It is recommended that you either set the rule to the defaults listed or that you clear Suspect IPs. While the use of an anonymizer does not necessarily indicate intent to commit a crime, it is highly suspicious because the user is masking their location. For example, users may be participating in marginal activities such as accessing gaming from a country where it is not allowed or accessing video or music content from a region that is not licensed. The hit rate for this rule is highly variable by customer because it is influenced by the portfolio of end users. However, the approximate review rate based on Anonymizers is 0.1% (one in 1000 transactions). False positive rates tend to vary greatly from as low as 20:1 for US and European users to as high as 100:1 for less developed regions.

Using the Negative IP Address List

The Negative IP Check Rule performs two functions within a single rule:

- The rule checks the IP addresses of end users against the list of known anonymizer proxies.
- The rule consults the Negative IP address list that you define to verify whether the IP is in one of the ranges defined in your table.

You can use the Manage List Data and Category Mappings page in Administration Console to add IP Addresses to the Negative IP address list. The rule performance for blacklisted IP addresses depends on how you manage your list. Typically, you add IPs to the list when you see fraudulent or risky access that you want to stop and you remove IPs from the list when a legitimate user requests for the same.

Note: You can review the transaction report to determine why an end user was blocked or challenged.

Appendix D: Summary of Server Refresh and Restart Tasks

Many configuration changes that you make might need the server to be restarted. 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 either restarted or refreshed. In such cases, Administration Console prompts you to refresh or restart, as applicable.

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

The following table lists the server tasks that either need to be refreshed or restarted after you have made any configuration changes.

Task	Refresh	Restart
Configure UDS Connectivity	✓	
Configure UDS	✓	
Configure Attribute Encryption	✓	
Configure Custom Locales	✓	
Set Default Organization	✓	
Add Account Type	✓	
Update Account Type	✓	
Delete Account Type	✓	
Add Custom Attributes for Account Type	✓	
Configure Email/Telephone Type	✓	
Configure Basic Authentication Policy	✓	
Enable Authentication and Authorization For Web Services	✓	
On the Instance Configuration page, updates to: ■ **Logging Configuration**: **Transaction Log Directory**, **Rollover After (in Bytes)**, **Transaction Log Backup Directory**, **Log Timestamps in GMT** ■ **Database Configurations**: **Minimum Connections**, **Maximum Connections**, **Increment Connections by**		✓

Task	Refresh	Restart
On the Instance Configuration page, updates to: ■ Instance Attributes ■ **Logging Configuration**: **Log Level**, **Enable Trace Logging** ■ **Database Configurations** (*except* **Minimum Connections**, **Maximum Connections**, **Increment Connections By**)	✓	
RiskMinder Connectivity	✓	
Trusted Certificate Authorities	✓	
Protocol Configurations		✓
Assign Channel and Default Account Type configurations	✓	
Create Ruleset	✓	
Add New Rules		
Update Rules	✓	
Delete Rules	✓	
Miscellaneous Configurations	✓	
Model Configuration	✓	
Callout Configuration	✓	
Migrate to Production	✓	
Create Organization	✓	
Update Organization	✓	
Create New Queue	✓	
Update Queue	✓	
Delete Queue	✓	

Appendix E: Multi-Byte Character and Encrypted Parameters

RiskMinder supports UTF-8, which is the variable width 8-bit encoding format of the universal Unicode encoding scheme. Variable-width encoding enables you to use varying number of bytes to encode a character set For information on configuring UTF-8, see the topic titled "Preparing for Installation" in the *CA RiskMinder Installation and Deployment Guide*.

RiskMinder also enables you to use hardware- or software-based encryption of your sensitive data.You can choose to encrypt sensitive parameters and also decide whether you want to display clear text data or encrypted data in Reports. The following table lists the parameters that can be selected for encryption and multi-byte character encoding. It also lists the keys used for the parameter and the level at which the key is applicable.

Parameter	IsEncrypted	HSM Support	KeyLevel	Key Type	IsMultiByte
UserName	Optional	Yes	Organization	OrgKey	Yes
User attributes	Optional	Yes	Organization	OrgKey	Yes
Configurations					
Action	No	No	None	None	No
OrgName	No	No	None	None	No
DeviceID	No	No	Global	Fixed - Internal	Yes
Device Signature	No	No	None	None	Yes
CALLERID	No	No	None	None	Yes
CONFIGNAME	No	No	None	None	No
CHANNELNAME	No	No	None	None	No
CLIENTIPADDRESS	No	No	None	None	No
AGGREGATORNAME	No	No	None	None	No
ASSOCIATIONNAME	No	No	None	None	No
ACCOUNTTYPE	No	No	None	None	No
MATCHEDRULE	No	No	None	None	No

Parameter	IsEncrypted	HSM Support	KeyLevel	Key Type	IsMultiByte
LINESPEED	No	No	None	None	No
CONNECTIONTYPE	No	No	None	None	No
ANONYMIZERTYPE	No	No	None	None	No
IP_ROUTINGTYPE	No	No	None	None	No
Rule Mnemonic	No	No	None	None	No
Rule Name	No	No	None	None	Yes
Rule Description	No	No	None	None	Yes
ACCOUNTID	No	No	None	None	Yes
PARENTUSERID	No	No	None	None	Yes
ERROR MESSAGE	No	No	None	None	Yes
QUEUE NAME	No	No	None	None	No
QUEUE DESCRIPTION	No	No	None	None	Yes
CASENOTE	No	No	None	None	Yes
3DSecure Elements					
ACQ_BIN	No	No	None	None	No
MERCHANT_NAME	No	No	None	None	Yes
MERCHANT_ID	No	No	None	None	No
MERCH_COUN	No	No	None	None	No
MERCHANT_URL	No	No	None	None	No
XID	No	No	None	None	No
PURCHASE_DESCRIPTION	No	No	None	None	Yes
PAN	No	No	None	None	No
EXPIRY	No	No	None	None	No
MERCH_CAT	No	No	None	None	No
TERM_URL	No	No	None	None	No
PREVTXNDATA	No	No	None	None	No

The following table describes whether the parameter is case-insensitive and whether it is displayed in reports.

Parameter	Case Insensitive	Displayed in Reports
UserName	Yes	Yes
User attributes	Yes	Yes
Configurations		
Action	No	Yes
OrgName	No	Yes
DeviceID	No	Yes
Device Signature	No	No
CALLERID	No	No
CONFIGNAME	No	Yes
CHANNELNAME	No	Yes
CLIENTIPADDRESS	No	Yes
AGGREGATORNAME	No	Yes
ASSOCIATIONNAME	No	
ACCOUNTTYPE	No	Yes
MATCHEDRULE	No	Yes
LINESPEED	No	
CONNECTIONTYPE	No	
ANONYMIZERTYPE	No	Yes
IP_ROUTINGTYPE	No	
Rule Mnemonic	No	Yes
Rule Name	No	Yes
Rule Description	No	Yes
ACCOUNTID	No	Yes
ERROR MESSAGE	No	No
QUEUE NAME	No	Yes
QUEUE DESCRIPTION	No	Yes
CASENOTE	No	Yes
3DSecure elements		

Parameter	Case Insensitive	Displayed in Reports
ACQ_BIN	No	Yes
MERCHANT_NAME	No	Yes
MERCHANT_ID	No	Yes
MERCH_COUN	No	Yes
MERCHANT_URL	No	Yes
XID	No	No
PURCHASE_DESCRIPTION	No	No
PAN	No	No
EXPIRY	No	No
MERCH_CAT	No	No
TERM_URL	No	No
PREVTXNDATA	No	No

Appendix F: Currency Conversion

This appendix provides an overview of currency conversion and describes the schema of the ARRFCURRCONVRATES table. It includes the following topics:

- Understanding Currency Conversion (see page 420)
- Currency Conversion Table (see page 421)

Understanding Currency Conversion

You can use the Rule Builder to configure a rule that compares the transaction amount against a threshold amount specified in the rule. You can specify the threshold amount in the base currency set for the organization. If the transaction currency and the base currency are different, then the transaction amount is automatically converted from the transaction currency to the base currency of the organization.

A few rule operators in specific channels allow you to specify the threshold amount in multiple currencies, in addition to specifying it in the base currency of the organization. When such a rule is executed, the transaction currency is compared with the currencies in which the threshold amount has been specified. If a match is found, then the transaction amount is directly compared with the threshold amount in that currency. In this case, no currency conversion is required. However, if a match is not found, then the transaction amount is first converted to the base currency and then compared with the threshold set in the base currency.

Important! Setting one of the threshold amounts in base currency is mandatory.

The following examples illustrate how this feature works:

Example 1

You have configured a rule with threshold amounts in USD, JPY, and AUD, while the organization base currency is USD. The following scenarios explain how currency conversion takes place during various types of transactions:

- **Scenario 1**: A transaction is being conducted in USD. Because the transaction currency is the same as the organization's base currency, the specified threshold is used without any need for currency conversion.
- **Scenario 2**: A transaction is being conducted in JPY. Because JPY is one of the currencies in which the threshold amount has been specified, the transaction amount is directly compared with the threshold amount in JPY. No currency conversion is required in this scenario.
- **Scenario 3**: A transaction is being conducted in EUR. Because EUR is *not* one of the currencies in which the threshold amount has been specified, the transaction currency is first converted from EUR to USD. The threshold value specified in USD is used for the comparison.

Example 2

You have configured a rule with threshold amounts in GBP, JPY, and AUD, while the organization base currency is GBP. The following scenarios explain how currency conversion takes place during various types of transactions:

- **Scenario 1**: A transaction is being conducted in GBP. Because the transaction currency is the same as the organization's base currency, the specified threshold is used without any need for currency conversion.

- **Scenario 2**: A transaction is being conducted in JPY. Because JPY is one of the currencies in which the threshold amount has been specified, the transaction amount is directly compared with the threshold amount in JPY. No currency conversion is required in this scenario.
- **Scenario 3**: A transaction is being conducted in EUR. Because EUR is *not* one of the currencies in which the threshold amount has been specified, the transaction currency is first converted from EUR to USD and then from USD to GBP. The threshold value specified in GBP is used for the comparison.

Currency Conversion Table

The conversion data for all supported currencies is stored in the ARRFCURRCONVRATES table. The ARRFCURRCONVRATES table contains the currency conversion data that is used to compare Amount field values when the transaction currency and the base currency of the organization differ. The following table describes the columns in the ARRFCURRCONVRATES table.

Column	Description	Format
VERSION	Rate Version	Integer with a value of 1.
CURR_FROM	The 3-digit ISO currency code for the transaction currency from which Amount is converted.	Integer with values between 0 and 1000.
CURR_FROM_STR	The 3-character ISO currency code for the transaction currency from which Amount is converted.	String with exactly three characters.
CURR_TO	The 3-digit ISO currency code for the currency to which Amount is converted.	Integer with values between 0 and 1000.
CURR_TO_STR	The 3-character ISO currency code for the currency to which Amount is converted.	String with a maximum length of three characters.
CONV_RATE	The rate of conversion between CURR_FROM and CURR_TO or CURR_FROM_STR and CURR_TO_STR.	Real number.
DTCREATED	Date and time when the CONV_RATE value was created.	
CURR_NAME_AND_NOTES	Additional notes.	

Guidelines for Using the ARRFCURRCONVRATES Table

Apply the following guidelines when you use the ARRFCURRCONVRATES table:

- By default, there is no data in the ARRFCURRCONVRATES table. You must populate this table with values after deploying RiskMinder.
- The currency conversion rates should be specified as the conversion value for one unit of the specified CURR_FROM or CURR_FROM_STR and CURR_TO or CURR_TO_STR.
- The conversion rates in the ARRFCURRCONVRATES table should be loaded with the CURR_TO or CURR_TO_STR as USD only.
- If a particular currency conversion is required, for example from EUR to JPY, then the Amount would be first converted from EUR to USD using the conversion rate from EUR to USD, and then the reverse of the USD to JPY conversion rate would be applied to get the Amount in JPY.

Appendix G: Troubleshooting RiskMinder Errors

This appendix describes the troubleshooting steps, which will help you resolve the errors that you might face while using RiskMinder. The troubleshooting topics are classified based on different RiskMinder components, as follows:

- Administration Console Errors (see page 424)
- User Data Service Errors (see page 428)

Before you perform any troubleshooting tasks, check the RiskMinder log files to see if there were any errors. By default, all the log files are saved in the following directory:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

The following table lists the default log file names of the RiskMinder components.

RiskMinder Component	File Name	Description
RiskMinder Server	arcotriskfortstartup.log	This file records all the start-up (or boot) actions. The information in this file is very useful in identifying the source of the problems if the RiskMinder service does not start up.
	arcotriskfort.log	This file records all requests processed by the Server after its startup. All requests processed by the server.
Administration Console	arcotadmin.log	This file records the Administration Console operations.
User Data Service	arcotuds.log	This file records the User Data Service (UDS) operations.

Note: See "RiskMinder Logging" (see page 389) for detailed information on the RiskMinder log files.

Administration Console Errors

Problem:

I cannot log in to the Administration Console as the Master Administrator (MA). I see the following message:
`Administrator Account is locked.`

Cause:

You might have tried to authenticate with the wrong password for more than the allowed authentication attempts.

Solution:

Reset the authentication attempt count, also known as *strike count* to 0, by using the following script:

- For MS SQL Server
  ```
  update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
  USERID='MASTERADMIN';
  GO
  ```
- For Oracle
  ```
  update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
  USERID='MASTERADMIN'; commit;
  ```
- For MySQL
  ```
  update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
  USERID='MASTERADMIN';
  COMMIT;
  ```

Problem:

When I try to log in to Administration Console as the MA, I see the following error message:
`There was an internal server error while processing the database query. Please contact your database administrator.`

Cause:

The possible cause for this issue might be that all active datasources in the database pool have been exhausted.

Solution:

To resolve this issue, do the following:

1. Ensure that the database server is reachable.

2. Restart the database or the database listener
3. If the Administration Console and the RiskMinder Server are using the same database, then:
   a. Restart the RiskMinder service.
   b. Restart the browser.

Problem:

I do not remember the MA password. How do I reset the password?

Solution:

1. Locate the folder with the scripts for your database type. The default location is:
   - **For MS SQL:**

     Windows:
     `<install_location>\Arcot Systems\dbscripts\mssql`

     UNIX-Based:
     `<install_location>/arcot/dbscripts/mssql`
   - **For Oracle:**

     Windows:
     `<install_location>\Arcot Systems\dbscripts\oracle`

     UNIX-Based:
     `<install_location>/arcot/dbscripts/oracle`
   - **For MySQL:**

     Windows:
     `<install_location>\Arcot Systems\dbscripts\mysql`

     UNIX-Based:
     `<install_location>/arcot/dbscripts/mysql`

2. Run the arcot-masteradmin-password-reset-2.0.sql script by using the database vendor tools.

   The MA password in now reset to the default password, which is **master1234!**.

If the preceding procedure does not work, then you must contact the CA Support team to reset the MA password for you.

Problem:

I cannot access the RiskMinder pages from the **Services and Server Configuration** tab. I see the following error message.
`Unable to contact the servers at this point of time. Please try later.`

Solution:

Ensure the following:

1. RiskMinder Server is running.
2. Log in as Master Administrator (MA).
3. Ensure that the RiskMinder Server connectivity details are correct:
   a. Navigate to the **Services and Server Configurations** tab.
   b. Activate the **RiskFort** subtab.
   c. Click the **Connectivity Details** link and check whether the RiskMinder **Host** and **Port** information for the **RiskFort Administration Connectivity** is set correctly.

Problem:

When I try to log in to Administration Console, I see the following message.
`ErrorCode 500: Internal server error.`

Cause:

- Your browser cache might be full.
- Your application server timeout settings might need to be reset.

Solution:

Do the following:

1. Empty the browser cache of the browser you are trying to open the console in and try again.
2. If the message persists, then try opening the console by using a different browser.
3. Check the timeout settings for the application server container.
4. If the problem still persists, then open the arcotadmin.log file and search for the "Administration Console configured successfully." string.
5. If you do not find the "Administration Console configured successfully." string, then look for the last (error description) entry in the file, and take appropriate action.

Problem:

I get the following error quite frequently while performing Administration Console operations:
`An internal communication error was encountered. Please contact System Administrator or retry later.`

Cause:

There might be one or more browser add-ons that are interfering with Administration Console operations.

Solution:

Disable unnecessary add-ons in your browser and perform the operation again:

Problem:

UDS is up, but the Administration Console did not correctly deploy. I see the java.lang.ClassNotFoundException exception in the arcotadmin.log file:

Cause:

This issue occurs only if the WAR or EAR was not properly deployed or was corrupted.

Solution:

To resolve this, do the following:

1. Clean up the working directory of your application server.

   For example, on Apache Tomcat, this directory is called work.

2. Deploy the WAR or EAR file again.

User Data Service Errors

Problem:

I have created and activated an organization by using the Administration Console, but when I try to perform any RiskMinder configurations, I see the following error:
`Organization not found.`

Cause:

The possible causes might be:

- You started the RiskMinder Server service *before* you started UDS.
- You are trying to perform the task for a new organization that you created, but did not refresh the RiskMinder Server cache.

Solution:

Do the following:

1. If you started RiskMinder Server before UDS, then the RiskMinder Server logs indicate that the server was unable to connect with UDS. Always start the application Server (UDS) first, and then start the RiskMinder Server service.
2. Refresh the RiskMinder Server Cache.

   When you create a new organization by using Administration Console, *always* restart the RiskMinder Server cache.

Note: See "Creating and Activating Organizations" (see page 232) for more information.

Problem:

While searching for users and administrators, I see the following error message:
`There was an internal server error while communicating with User Data Service. Please contact your Administrator.`

Cause:

There might be too many users to be searched under given organization(s). As a result, the operation did not complete within the specified timeout.

Solution:

Do the following:

1. Log in to Administration Console as an MA.
2. Navigate to **Services and Server Configurations**, **Administration Console**, and then **UDS Connectivity Configuration** page.

3. On the Connectivity Configuration page:
   a. Increase the value of the **Connection Timeout** field.
   b. Increase the value for the **Read Timeout** field.
4. If the preceding steps do not work, then change the search criteria to narrow down the expected search results.