Arcot RiskFort™
Installation and Deployment Guide
(for Windows Platforms)
Version 2.2.6

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot RiskFort Installation and Deployment Guide
Version 2.2.6
September 2010
Part Number: RF-0226-0IGW-10

Trademarks

Patents

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

Third Party Software

All the third-party software used by RiskFort and related components are listed in the appendix “Third-Party Software Licenses”.

Contents

Preface

The Arcot RiskFort Installation and Deployment Guide covers the following topics:

- Overview of Arcot RiskFort
- RiskFort installation instructions
- RiskFort SDK and Web Services configuration
- RiskFort uninstallation instructions
- RiskFort fast-growing tables and database-sizing recommendations
- RiskFort configuration files

Intended Audience

This guide is intended for administrators, system operators, and other users who are responsible for the installation and deployment of Arcot RiskFort.

To install and configure Arcot RiskFort on Windows successfully, the account that you plan to use for installation must belong to the `Administrators` group.

Note: Some topics in this guide are intended for users who are comfortable running system administration operations, such as creating users and groups, adding users to groups, and installing operating system patches. If you are not familiar with these tasks, Arcot strongly recommends that an experienced system operator or database administrator performs them.

Information Included in this Guide

This guide is organized in parts as follows:

- Chapter 1, "Understanding RiskFort Basics", describes the features and the architecture of RiskFort.
- Chapter 2, "Planning the Deployment", briefly discusses the various models that can be deployed for RiskFort.

- Chapter 3, "Preparing for Installation", discusses the requirements for installing RiskFort on Windows. It also provides configuration and planning-related information.
- Chapter 4, "Deploying RiskFort On a Single System", guides you through the steps for installing RiskFort in a single-system environment.
- Chapter 5, "Deploying RiskFort on a Distributed System", guides you through the steps for installing RiskFort in a distributed-system environment.
- Chapter 6, "Configuring RiskFort SDKs and Web Services", describes the steps to configure the APIs and Web services provided by RiskFort on Windows.
- Chapter 7, "Uninstalling RiskFort", guides you through the steps for uninstalling RiskFort and related components on Windows.
- Appendix A, "RiskFort Directory Structure", provides the information about the location of the files that are installed by the RiskFort installer.
- Appendix B, "Configuration Files and Options", discusses the configuration files that RiskFort uses and the parameters that you must configure in these files. It also includes samples of these default configuration files.
- Appendix C, "Database Reference", discusses the fast-growing RiskFort tables and their trimming recommendations.
- Appendix D, "Default Port Numbers and URLs", lists the default port numbers and URLs that RiskFort uses.
- Appendix E, "Configuring Application Server for Database Connection Pooling", describes the application server configuration that must be made for connection pooling.
- Appendix F, "Configuring SSL", describes how to set up SSL communication between RiskFort Server and its components.
- "Third-Party Software Licenses", lists the third-party software packages that are used by RiskFort.
- "Glossary", lists the key terms related to RiskFort.

Related Publications

Other related publications include:

Arcot RiskFort 2.2.6 Administration Guide	This guide includes the information to administer and configure RiskFort.

Arcot RiskFort 2.2.6 Java Developer's Guide	This guide describes the Java APIs provided by RiskFort and also explains how to use them
Arcot RiskFort 2.2.6 Quick Installation Guide	This guide provides a summary of the tasks required to install RiskFort.

Conventions Used in This Book

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

Typographical Conventions

This manual uses the following typographical conventions:

Italic	Emphasis, Guide names
Bold	User input, GUI screen text
`Fixed`	File and directory names, extensions, Command Prompt, CLI text, code in running text
`Fixed Bold`	Target file or directory name in the path
`Fixed`	Command Prompt, CLI text, code
`Fixed-Italic`	File or directory name that might be different from user to user
Link	Links within the guide, URL links

Formats

This manual uses the following formats to highlight special messages:

	**Note:** Highlights information of importance or special interest.

	**Tip:** Highlights a procedure that will save time or resources.

	**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.

	**Important:** Information to know before performing an operation.

	**Caution:** Makes the user attentive of the possible danger.

	**Book:** Provides reference to other guides.

Contacting Support

If you need help, contact Arcot Support as follows:

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

Chapter 1
Understanding RiskFort Basics

Arcot RiskFort (referred to as RiskFort later in the guide) is an adaptive authentication solution that evaluates each online transaction (shopping, banking, or corporate access) in real time by examining a wide range of collected data against the out-of-box rules. It then assigns each transaction a risk score and advice. The higher the risk score, the greater the possibility of a fraud. Based on your business policies, your application can then use this risk score and advice to approve or decline the transaction, ask for additional authentication, or alert a customer service representative.

RiskFort is highly configurable, and offers you the flexibility to modify the configuration parameters of any of the risk evaluation rules in keeping with your policies and risk-mitigation requirements. It also gives you the flexibility to modify the default risk score, scoring configuration, and scoring priorities of individual rules and selectively enable or disable the execution of one or more rules.

Besides pre-configured out-of-the-box rules, RiskFort's field-programmable Add-On rules capability enables you to selectively deploy your industry-specific rules.

This chapter introduces you to the basic concepts of RiskFort, explains its architecture, and then walks you through the features and enhancements that have been introduced in this release:

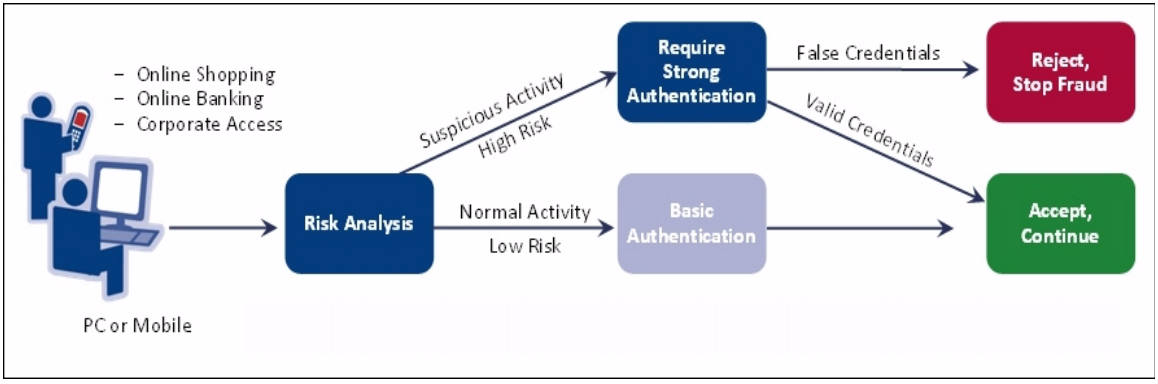
Introduction to RiskFort

RiskFort collects a wide range of data for risk evaluations (as discussed in "Data Used for Risk Evaluations".) This data is then evaluated with the help of configured rules (see "Rules and Risk Processing".) The result of each rule is then evaluated in the order of priority set by a RiskFort administrator and a score and advice is generated corresponding to the first rule that matched ("Risk Score and Advice".) RiskFort then creates an user-device association in the RiskFort database ("User-Device Associations".)

How RiskFort Works

Figure 1-1 illustrates how RiskFort broadly assesses risk and detects fraud for each transaction.

Figure 1-1 Pre-Login Risk Assessment and Fraud Detection



You can implement RiskFort's risk analysis capability either *before* the user logs in your online application or *after* they have successfully logged in, as discussed in the following sub-sections.

Pre-Login Risk Assessment and Fraud Detection

When a user accesses your online application, you can assess them for potential risk even before they log in.

If you call RiskFort's risk analysis capability even before a user logs in to your online application, then the risk evaluation workflow is as follows:

1. User accesses your online application.
2. Your application calls RiskFort to analyze the risk associated with the transaction.
3. RiskFort evaluates the risk using the incoming inputs and the configured rules. It uses the data discussed in section "Data Used for Risk Evaluations" for the purpose.
4. Based on the result of rules that were executed and whether the assessed information matched, RiskFort generates a Risk Score and Advice.
5. Your application validates the user, given:
   - If the risk is low, then the user is allowed to access your online application.
   - If the risk is high, then the user is denied access to your system.

- If the transaction is tagged as suspicious, your application challenges the user for additional (secondary) authentication to prove their identity.

Post-Login Risk Assessment and Fraud Detection

When a user accesses your online application, you can first log them in and then comprehensively assess them for potential risks when they try to perform pre-defined actions (such as wire transactions.)

If you call RiskFort's risk analysis capability *after* you authenticate a user in to your online application, then the risk evaluation workflow is as follows:

1. User logs into your online application.
2. User tries to perform certain actions identified by you.
3. Your application calls RiskFort to analyze the risk associated with the transaction.
4. RiskFort evaluates the risk using the incoming inputs and the configured rules. It uses the data discussed in section "Data Used for Risk Evaluations" for the purpose.
5. Based on the result of rules that were executed and whether the assessed information matched, RiskFort generates a Risk Score and Advice.
6. Your application allows the user to continue with the transaction, given:
   - If the risk is low, then the user is allowed to continue.
   - If the risk is high, then the user is denied the transaction.
   - If the transaction is tagged as suspicious, your application challenges the user for additional (secondary) authentication to prove their identity.

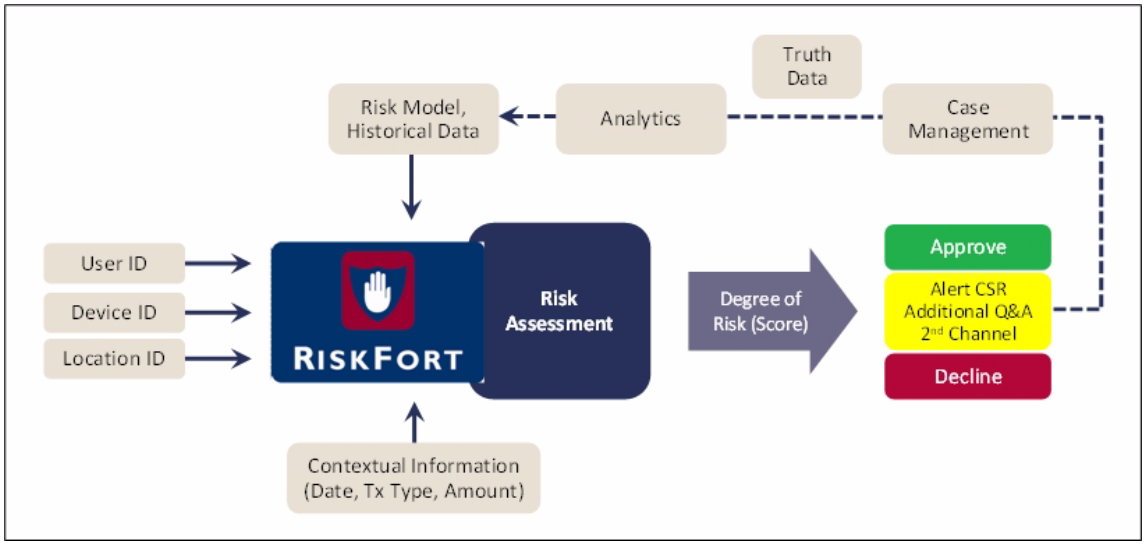
Data Used for Risk Evaluations

RiskFort bases the result of a risk analysis by comparing the following incoming information, if available, with the historical data for the user:

- Fraud Model
- Device DNA
- Device ID
- Location Information
- User and Transaction Information

Figure 1-2 illustrates how RiskFort uses this data. The following subsections provide a quick overview of each of the data category.

Figure 1-2 Data Used by RiskFort



Fraud Model

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

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

Device DNA

Device DNA (also referred to as Device fingerprinting or PC fingerprinting in industry terms) is a tagless device identification and analytics technique used for gathering and analyzing user's system information (such as browser, operating system, installed softwares, screen display settings, multimedia components, and other attributes) to generate a risk profile of a device in real-time.

Some of the MFP attributes collected by RiskFort from the end user's device include:

- Operating system name and version
- Browser information (such as name, major version, minor version, JavaScript version, HTTP headers)
- Screen settings (such as height, width, color depth)
- System information (such as time zone, language, system locale)

For every transaction by the end user, RiskFort matches the corresponding MFP stored in its database with the incoming information. If this match percentage (%) is equal to or more than the value specified in the Other Configuration screen of the Administration Console, then it is considered "safe".

Device ID

The *Device ID* is a cookie that RiskFort generates and sets on the end user's system to identify and track the device used for logging into your online application and performing transactions. The information is in encrypted format.

The RiskFort Device ID can be stored as:

- **Flash object:** Flash Shared Object (FSO) stored with `.sol` or `.ssl` (if SSL is being used for communication) extension, available in the Flash Player directory of the user's profile. This type of cookies are common across all browsers.
- **Browser cookie:** HTTP cookie whose extension and storage location depends on the browser used by the end user. This type of cookies are browser-specific.

Note: Device ID is *not* available to RiskFort the first time it evaluates a device. This data is used in subsequent evaluations.

When a user is evaluated by RiskFort for the first time, RiskFort generates unique device information (Device ID) in the form of a cookie and sets it on the user's system. Every subsequent time the user is assessed, RiskFort verifies if the Device ID on user's system matches with the Device ID stored in RiskFort database. If the two Device IDs match, the incoming information is considered "safe".

Location Information

Derived from end user's system IP address, this information includes geo-location information such as, Locale, ISP, time zone, and related geographical information. RiskFort integrates with Quova® for this information, who provide 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

For every transaction by the end user, RiskFort matches the incoming IP address and the information derived from this IP address with the related information stored in the RiskFort database. This information is then used as an input for Negative IP Address List, Negative Country List, and Zone Hopping rules.

User and Transaction Information

Typically, a user's login ID identifies a user uniquely in the system. RiskFort uses this information as one of the attributes to identify a user uniquely.

In addition, if configured, RiskFort can also accept contextual or transaction information (such as transaction amount, transaction type, and date) for analyzing the risk associated with a transaction. However, you must use custom Add-On rules to enable RiskFort to evaluate this contextual information.

Book: See the *Arcot RiskFort 2.2.6 Administration Guide* for more information on Add-On rules.

Rules and Risk Processing

After the required data is collected, it is forwarded to *Rules Engine* (a module of RiskFort Server). The Rules Engine is a set of configured rules that evaluate this information based on incoming information and historical data, if available.

A *rule*, in turn, is a condition or a set of conditions that must be true for a rule to be invoked. By default, each rule is assigned a priority and is evaluated in the specific order of its priority level. However based on your business requirements, you can change this priority of rule scoring.

The out-of-box rules provided by RiskFort are explained in Table 1-1.

Table 1-1. Out-of-Box RiskFort Rules

Rule Name	Description
Trusted IP	Transactions originating from IP addresses “trusted” to the organization receive a low score, by default, and the advice is `Allow`.
Trusted Aggregator	Many enterprises use the services of account and data aggregation service providers to expand their online reach. The originating IP addresses when users log in from a protected portal versus when they come in through such aggregators are different. Transactions originating from aggregators “trusted” to the organization receive a low score, by default, and the advice is `Allow`.
Negative IP	This list constitutes the IP addresses that originate from anonymizer proxies or have been the origin of known fraudulent or malicious transactions in the past. Transactions originating from configured negative IP addresses receive a high score and the advice is `Deny`.
Negative Country	This list comprises the countries that have been known to be origins of significant number of frauds in the past. RiskFort derives the country information based on the input IP address, and then uses this data to return a high risk score for online transactions originating from these "negative" countries.
User Velocity	Frequent use of the same user ID could be an indication of risky behavior. For example, a fraudster might use the same user ID and password from different devices to watch a specific activity in a targeted account. Too many transactions originating from the same user within a short (configurable) interval receive a high score and the advice is `Deny`.
Device Velocity	Frequent use of the same device could also be an indication of risky behavior. For example, a fraudster might use the same device to test multiple combinations of user IDs and passwords. Administrators can now configure RiskFort to track for this behavior, as well. Too many transactions originating from the same user device within a short (configurable) interval receive a high score and the advice is `Deny`.
Zone Hopping	If a user logs in from two long-distance locations within a short time span using the same user ID, this might be a strong indication of fraudulent activity. In addition, a User ID can also be shared, in which case, RiskFort understands that the two people sharing the same User ID can be in geographically different locations and responds with appropriate response. Transactions originating from the same user from very large distances within a short (configurable) interval receive a high score and the advice is `Deny`.

Table 1-1. Out-of-Box RiskFort Rules

Rule Name	Description
Unknown User	A *known user* is already registered in the RiskFort database. If the user is unknown to RiskFort, then by default an `Alert` is returned. The CSR can then choose to further authenticate the user based on the advice.
Exception User	An organization may choose to exclude a user from risk evaluation during a certain time interval. For example if a user travels to a country that is configured as negative in RiskFort, then for the specified interval their status can be changed to an *exception user*. RiskFort returns a low risk score for transactions originating from exception users and the advice is typically `Allow`.
DeviceID	The Device ID is a device identifier string that RiskFort generates and stores as a cookie on the end user's system to identify and track the device that the end user uses for logging into your online application and perform transactions. RiskFort returns a low risk score for transactions originating from known devices and the advice is typically `Allow`.
User Associated with Device and Device-MFP Matched	Transactions originating from a known device whose MFP matches and the user is associated with the current device receive a low score, and the advice is `Allow`.
Device-MFP Matched but User Not Associated with Device	Transactions originating from a known device that is not associated with a known user receive a medium score, and the advice is `IncreaseAuth`.
User Associated with Device but Device-MFP Does Not Match	Transactions originating from a known device whose MFP did not match receive a medium score, and the advice is `IncreaseAuth`.
User Not Associated with Device and Device-MFP Does Not Match	Transactions originating from an unknown device that is not associated with a known user receive a high score, and the advice is `Deny`.

Rules Engine executes these rules in the order of their precedence. The evaluation result is then forwarded to another module of RiskFort Server called the Scoring Engine.

Risk Score and Advice

Based on the result of the execution of each rule that Rules Engine provides, the *Scoring Engine* evaluates the score of each rule in the order of priority set (by the administrator) and returns the score corresponding to the first rule that matched.

For example, consider that you have configured three rules in the following order:

1. Negative IP (say, with a score of 85)
2. User Velocity (say, with a score of 70)
3. Device Velocity (say, with a score of 65)

Note: High scores are typically assigned to rules that are more critical.

If RiskFort determines that a transaction is coming from a negative IP address, then it returns a score of 85 (Deny), based on the first configured rule that matched. If another transaction exceeds the configured Device Velocity, then RiskFort returns a score of 65.

The *risk score* generated by the Scoring Engine is an integer from `0` through `100` (Table 1-2). RiskFort then uses this risk score to generate the corresponding *advice* and returns this advice to your application.

Table 1-2 shows a sample risk score and corresponding advice matrix.

Table 1-2. Risk Score - Advice Matrix

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

Based on the data received by RiskFort, this advice can be one of the following:

- **ALLOW:** RiskFort returns `ALLOW`, if the risk score associated with the transaction is low.
- **ALERT:** If a user who is not registered with RiskFort tries to log in, then `ALERT` is returned.

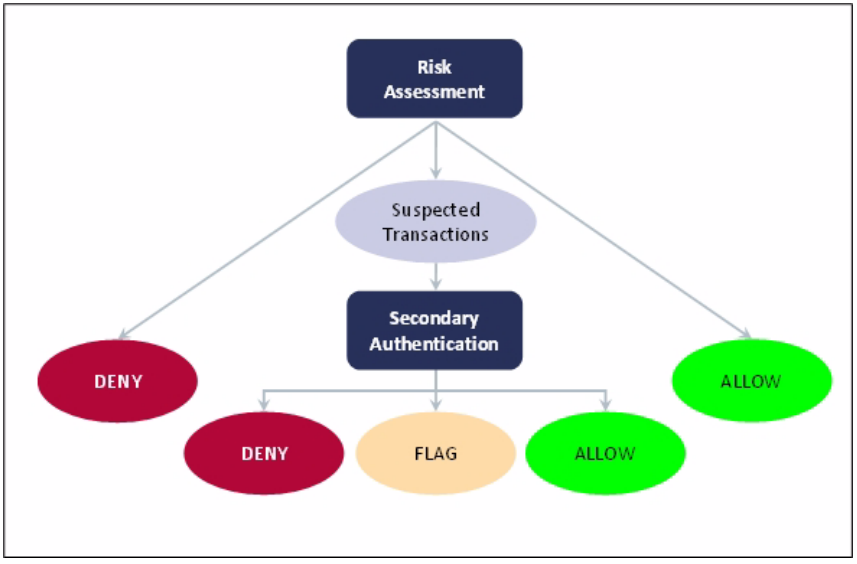
- **INCREASE AUTHENTICATION:** When RiskFort detects a suspicious transaction, it flags the transaction with `INCREASE AUTHENTICATION` and advises the application to force the user for additional authentication.

  For example, when a user registered with RiskFort attempts a transaction from a device that is not yet recognized by RiskFort, then the user must undergo secondary authentication (such as OTP or QnA) with your application.

- **DENY:** RiskFort returns the `DENY` advice when high risk score is associated with the transaction.

Figure 1-3 illustrates the advices returned by RiskFort

Figure 1-3 Risk Advices



User-Device Associations

For future evaluations, RiskFort uniquely identifies a user as a valid user by automatically associating (or binding) a user to the device that they use to access your application. This is referred to as an *association* (or device binding) in RiskFort terminology. Users who are not bound are more likely to receive an advice of Increase Authentication in order to be authenticated.

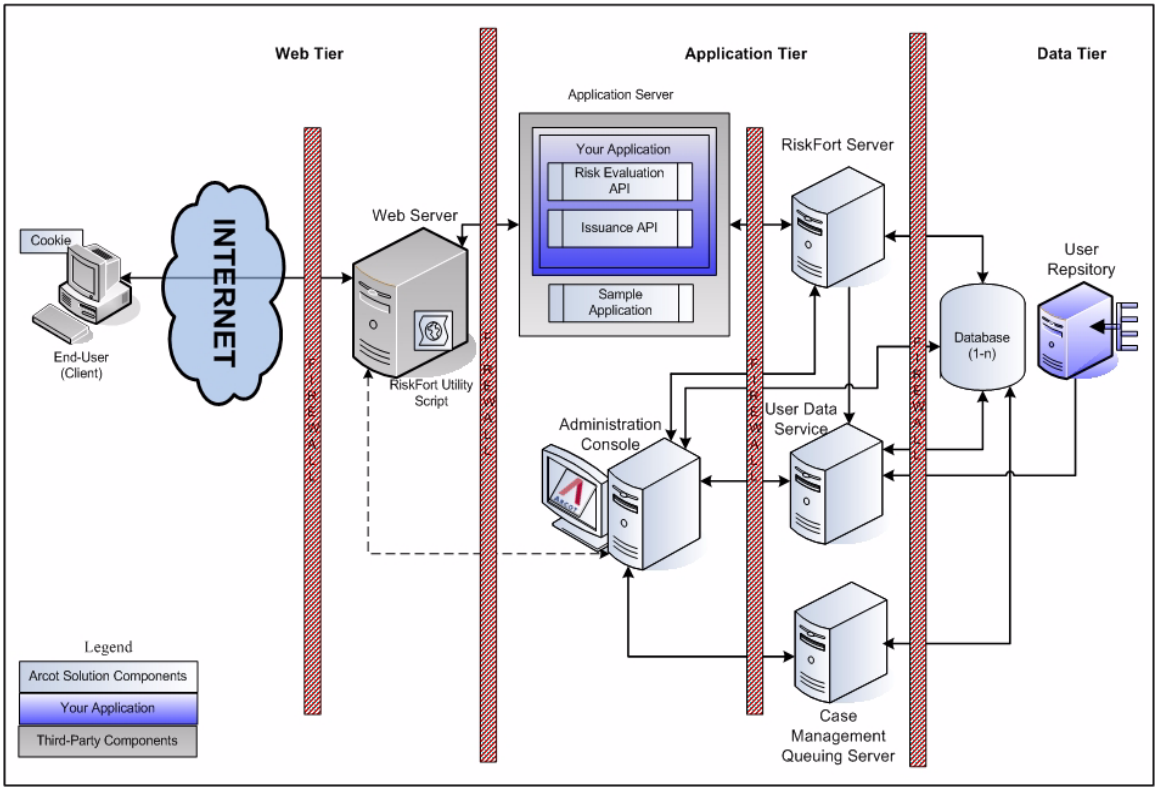
RiskFort also allows users to be bound to more than one devices. For example, a user can use a work and a home computer to access your application. Similarly, you can bind a single device to more than one users. For example, members of a family can use one computer to access your application.

RiskFort Architecture

You can install RiskFort on a single system or you can distribute its components across multiple systems, as discussed in later chapters in the guide. However to ensure maximum security and integrity of data and transactions, Arcot recommends the architecture shown in Figure 1-4 with the following three layers:

- Web Tier
- Application Tier
- Data Tier

Figure 1-4 Recommended Three-Tiered RiskFort Architecture



The following subsections discuss the components of these layers.

Web Tier

This layer comprises the HTML content and interacts directly with the user over a network or the Internet.

The *RiskFort Utility Script* (`json.js`), which is a client-side JavaScript and must be included in your application, is served to the end user's browser through the Web servers that reside in this layer. This script enables you to:

- Set the Device ID (in form of a cookie) on the end user's system.
- Collect the Device DNA (MFP) information and Device ID information.

Book: See Chapter 5, "Collecting Device ID and DeviceDNA" in the *Arcot RiskFort 2.2.6 Java Developer's Guide* for detailed information on MFP, Device ID, and using the utility script.

Application Tier

This layer constitutes all application server components in the system. These include RiskFort Server, UDS, Administration Console, and the RiskFort SDKs:

Note: All components in this layer can be installed on one system or can be distributed across multiple systems, as discussed in Chapters 2, 3, and 4.

- **RiskFort Server**

  Server component that processes risk evaluation requests from your application through RiskFort SDKs.

- **Case Management Queuing Server**

  Server component that schedules and dispatches cases to Customer Support Representatives (CSRs) and subsequently manages the lifecycle of these cases.

- **Administration Console**

  Web-based console for configuring server instances, communication mode between RiskFort components, business rules and the corresponding data, and for managing organizations, administrators, and users.

- **User Data Service**

  The abstraction layer that provides access to user- and organization-related data from different types of user repositories, such as relational databases (RDBMSs) and directory servers (LDAPs).

- **Risk Evaluation SDK**

  APIs that can be invoked by your application to forward risk-analysis requests to RiskFort Server.

- **Issuance SDK**

  APIs that can be invoked by your application to forward issuance requests to RiskFort Server for enrolling users and for managing user details in RiskFort.

- **Sample Application**

  Sample Application demonstrates the usage of RiskFort Java APIs and how your application can be integrated with RiskFort. The Sample Application can also be used to verify if RiskFort was installed successfully, and if is able to perform risk-evaluation and issuance operations.

Data Tier

This layer comprises the instances of relational databases that store the configuration, user, and historical data used by RiskFort to analyze each transaction. In addition, this layer also constitutes any directory servers (LDAPs) that you have configured for storing user details.

What's New in this Release

The key features and enhancements in the RiskFort 2.2.6 release include:

- Infrastructure for Supporting Multiple Channels
- Provision of Feedback to the Predictive Model During Post-Evaluation
- Enhancements in the Case Management Module
- Support for SSL-Based Communication Between the RiskFort Components and the Database
- Support for Vendor-Specific ODBC Drivers on Windows Platform
- Administration Web Services Previously Exposed as WAR File Now Moved to RiskFort Server
- Enhanced Amount Check Rule Type Configuration

Infrastructure for Supporting Multiple Channels

By default, RiskFort is shipped with support for two channels - DEFAULT and 3D Secure. However, in this release the infrastructure has been enhanced to support any required channel.

If a new channel is required, then Arcot can provide the new on-demand schema based on the type of data relevant for the new channel.

Provision of Feedback to the Predictive Model During Post-Evaluation

From this release, RiskFort can now send feedback information to the Predictive Model during the Post-Evaluation phase.

Enhancements in the Case Management Module

In the preceding release (2.1), every user transaction (login, wire transfer, or any transaction that your application was evaluating risk for) was considered as a potential *case*. However in this release, **a case is generated when:**

- The advice for the risk evaluation for a transaction is either **Increase Authentication** or **Deny**.

Note: If there was already an open case for the user, then this transaction is added to the existing case.

- A user contacts your Call Center to dispute a transaction.

  In this case, the 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: For each of these transactions if a case is already open for the given user, then these transactions are added to the existing case.

Three distinct roles are now supported in Case Management:

- **Queue Managers:** Specify Case Queue configuration, assign CSRs to the Queue, and determine the order of cases within the Case Queue in which the operators must work on the cases. Additionally, QMs can view statistics on the managed and pending cases.

Note: This release supports only one Queue, the Default Queue, for each organization in the system.

- **Customer Support Representatives (CSRs):** Responsible for:
  - Attending customer calls. For example, a customer might call to dispute a transaction. In such cases, CSRs record the input from the customer and take action accordingly, The recorded information can then be used for analysis by Fraud Analysts to tune RiskFort.

    If further action needs to be taken on the case, CSRs can also specify when the user must be contacted next.

    Based on the user input, CSRs can also add users to the Exception User List for a specified duration.
  - Calling customers to confirm the authenticity of a suspect transaction. Based on the end user input, they can also add the users to the Exception User List for a specified duration.

Note: They are allocated cases automatically when they log in and/or go to the next case.

- **Fraud Analysts:** Analyze the trends in transactions by using the truth data collected by other operators and available filters. If the transaction set is large, they can also export the data offline and then analyze them. Based on their analyses, they can advise the system administrators on fine-tuning RiskFort.

  If the Fraud Analyst suspects a transaction to be suspicious, they can raise a request for operators to call the end user and find more details related to the suspect transactions even if the system had not suspected those transactions.

  This release provides a number of filters that the Fraud Analysts can use to analyze the transaction data. These include capability to display:
  - Transactions within the specified time range
  - Transactions in the last 30 minutes, 1 hour, and so on.
  - Transactions with the specified risk advice.

- Transactions where a certain rule kicked in.
- Transactions where the secondary authentication status is either Successful, Failed, or Unknown.
- Transactions from the same Device, Merchant, IP address, or User.
- (Specific to 3-D Secure) Transactions where the Merchant Name begins with or ends with a specified pattern or contains a specified word.

Support for SSL-Based Communication Between the RiskFort Components and the Database

All components communicating with the RiskFort Database now support two-way SSL communication. These include:

- RiskFort Server
- Administration Console
- User Data Service
- Case Management Queuing Server

Support for Vendor-Specific ODBC Drivers on Windows Platform

On Windows, RiskFort can now be configured to use the ODBC DSN that uses vendor-specific ODBC drivers.

Administration Web Services Previously Exposed as WAR File Now Moved to RiskFort Server

The following Administration Web services that were earlier exposed as a WAR file have now been built into the RiskFort Server:

- `addUserToExceptionList`
- `deleteUserFromExceptionList`
- `getUserProfile`
- `getLocationAndConnectionInfo`

Important: The Namespace has changed. Therefore if you want to use these built-in Web services, then you must rebuild their stub. However, no code change is required.

The `wsdls\admin\` directory in `ARCOT_HOME` contains the accompanying WSDL (`ArcotRiskFortAdminWebService.wsdl`) that can be used to generate the Web Services client code to communicate with the RiskFort Web Services.

Enhanced Amount Check Rule Type Configuration

The comparison operators for the Amount Check rule type configuration are now available as a drop-down when an Amount Check Add-On rule type is configured. The supported operators include:

- `EQUAL TO`
- `NOT EQUAL TO`
- `GREATER THAN OR EQUAL TO`
- `LESS THAN OR EQUAL TO`
- `GREATER THAN`
- `LESS THAN`

Book: See the *Arcot RiskFort 2.2.6 Administration Guide* for more information on this change.

Chapter 2
Planning the Deployment

This chapter will help you to select a deployment model, and determine which RiskFort components and prerequisite software to install on each system. Architecture diagrams for each deployment model are also provided to assist you with planning.

Note: In this guide, *System* refers to a physical device and *Server* refers to software that is run on the system.

The chapter covers the following topics:

Deployment Overview

This section provides a quick overview of steps for deploying RiskFort and provides pointers for choosing a deployment model based on your requirements:

1. Choose a deployment model. RiskFort can be installed on a single system or across multiple systems.

   See "Choosing a Deployment Model" for more information.

2. Ensure that the system where you plan to install RiskFort and its components meets all hardware requirements.

   See "Hardware Requirements" on page 3-33 for more information.

3. Install the prerequisite softwares.

   See "Software Requirements" on page 3-34 for more information.

4. Create a database user in the SQL database.

   See "Configuring Database Server" on page 3-36 for more information.

5. Install RiskFort:

   - See "Performing Complete Installation" on page 4-44 for more information on installing in a single-system environments.
   - See "Installing on the First System" on page 5-74 for more information on installing in a distributed environments.

6. Run SQL scripts in the database to create the Arcot schema and set initial configuration preferences:

   - See "Running Database Scripts" on page 4-52 for more information on running SQL scripts for single-system deployments.
   - See "Running Database Scripts" on page 5-84 for more information on running SQL scripts for distributed deployments.

7. Deploy User Data Service (UDS) and Administration Console:

   - See "Deploying Web Applications" on page 4-53 for more information on deploying and starting UDS and Administration Console for single-system deployments.
   - See "Deploying Web Applications" on page 5-85 for more information on deploying and starting UDS and Administration Console for distributed deployments.

8. Log into the Administration Console as a Master Administrator and initialize the console:

   - See "Logging in to Administration Console" on page 4-60 and "Bootstrapping the System" on page 4-60 for more information on initializing the Administration Console for single-system deployments.
   - See "Logging in to Administration Console" on page 5-91 and "Bootstrapping the System" on page 5-92 for more information on initializing the Administration Console in a distributed environment.

9. Start the RiskFort Server and the Case Management Queuing Server, and verify that the services are coming up correctly:

   - See "Starting RiskFort Server" on page 4-66, "Starting the Case Management Queuing Server" on page 4-66, and "Verifying the Installation" on page 4-67 for more information on initializing the Administration Console for single-system deployments.
   - See "Starting RiskFort Server" on page 5-98, "Starting the Case Management Queuing Server" on page 5-98, and "Verifying the Installation" on page 5-99 for more information on initializing the Administration Console in a distributed environment.

10. (**For Distributed Installation Only**) Install RiskFort on the subsequent system(s):
    - See "Installing on the Second System" on page 5-100 for more information.
11. Deploy and run the Sample Application to test RiskFort installation:
    - See "Deploying Sample Application" on page 4-68 and "Using Sample Application" on page 4-69 for more information on doing this in a single-system environments.
    - See "Deploying Sample Application" on page 5-101, "Configuring Sample Application for Communication with RiskFort Server" on page 5-102, and "Using Sample Application" on page 5-103 for more information on doing this in a distributed environment.

Choosing a Deployment Model

As a part of RiskFort deployment, RiskFort Server is the primary component that you must install. This is because, it provides the risk evaluation service, which includes transaction risk evaluation. Your applications that need to use RiskFort Server can integrate with it by using Java SDKs or Web Services shipped along with it.

RiskFort also requires an SQL database for storing server configuration data, user-specific preferences, and usage data.

Typically, all RiskFort components are installed on a single system for development and simple testing. However, in production deployments and staging environments, RiskFort Server should be installed on its own system. The shipped SDKs or Web Services are installed on a different system or systems that contain the application that users log in to.

RiskFort is also shipped with Sample Application, which can be used to verify that RiskFort is installed properly and is able to perform risk evaluation. Sample Application also serves as a code sample for integrating RiskFort with your existing application(s).

The high-level deployment types supported by RiskFort are:

- **Single-System Deployment** - For development or testing
- **Distributed-System Deployment** - For production or staging environments
- **High-Availability Deployment** - For high availability and scalability, production, or staging environments

Deploying on a Single System

In a single-system deployment, all components of RiskFort and the application, which users log in to, are installed on a single system. The database might be on the same system where RiskFort is installed, or on a different system.

This deployment model is typically used for development, proof of concept, or initial testing.

It is possible to use both Java SDKs and Web Services in a single-system deployment. The prerequisite software for these components are identical.

The simplest way to perform a single-system deployment is to choose the **Complete Installation** (see "Performing Complete Installation" on page 4-44 for more information) option while running the RiskFort installer.

Component Diagrams

The diagrams in this section depict possible deployment options for prerequisite software and RiskFort components. Note, that if you perform a **Complete Installation**, then both Java SDKs and Web Services will be present on the system. You can choose to use one or both integration methods, in this case.

- Deploying Java SDKs
- Deploying Web Services

If you plan to perform a single-system deployment, then you must make the following decisions:

Decision Points

- Install a database server on the system which has RiskFort Server, or use an existing database on a separate system.
- Use Sample Application or write your own Web application.

	**Important:** Sample Application must *not* be used in production deployments. Arcot strongly recommends that you build your own Web application by using Sample Application as a code-reference.

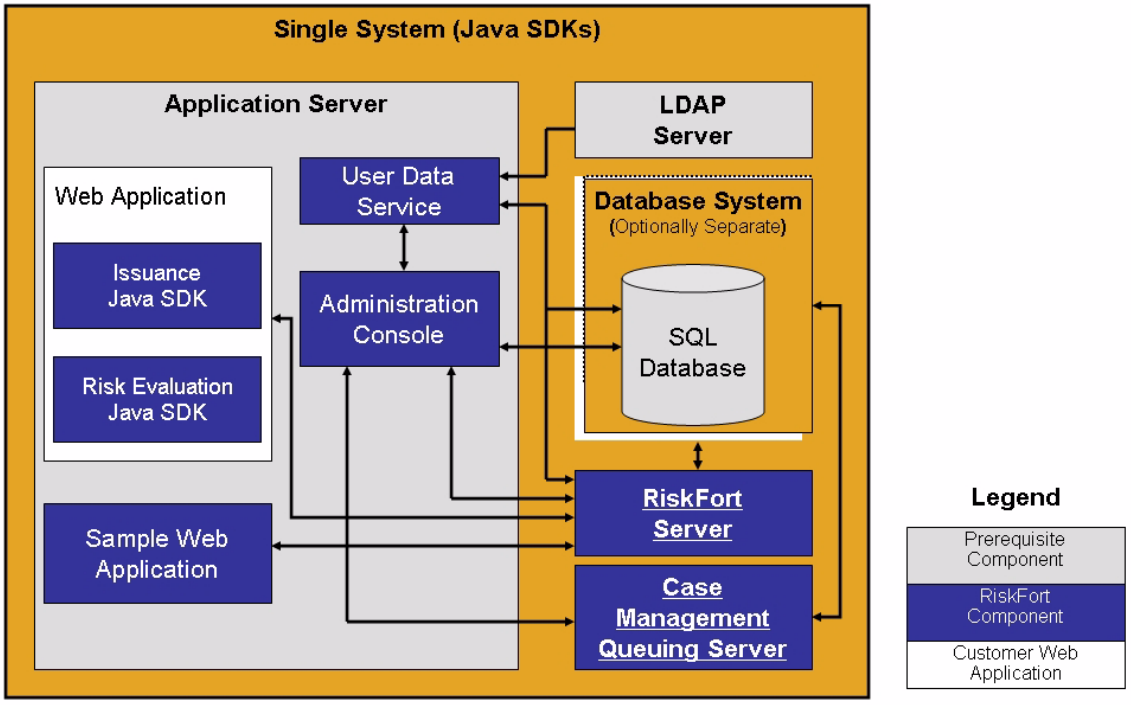
- Use Java SDKs or Web Services to integrate with your own Web application.

The following sections will help you to achieve your deployment decision.

Deploying Java SDKs

Figure 2-1 illustrates RiskFort Server and Java SDKs deployed on a single system.

Figure 2-1 RiskFort (Java SDKs) on a Single System



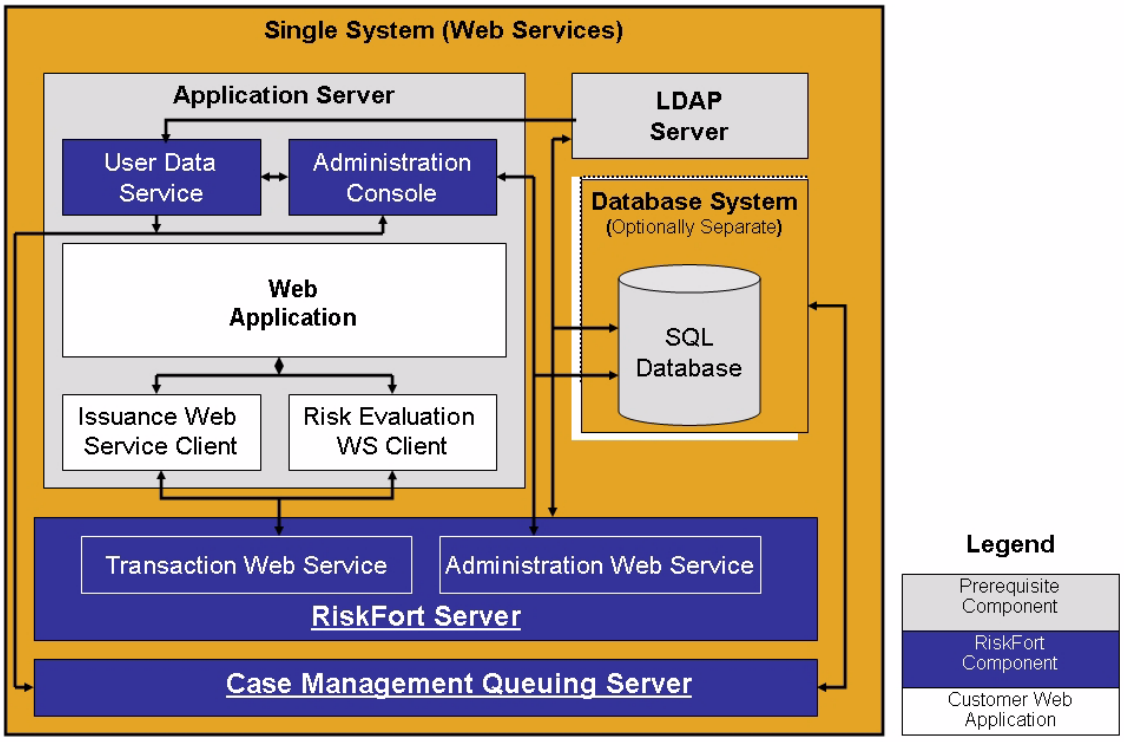
Note: The use of a Web server to deliver HTML pages for the application server is optional and is transparent to RiskFort. In production deployments, this approach is generally used to improve Application Server performance and security. Refer to the documentation of your Application Server for detailed information.

Deploying Web Services

If you plan to deploy Web services, then Figure 2-2 illustrates RiskFort Server and Web Services on a single system.

Note: Because all Web Services are now built into the RiskFort Server module itself, you just need to install the RiskFort Server on the target system and generate the requisite client stubs. No further configuration is required.

Figure 2-2 RiskFort (Web Services) on a Single System



Deploying on Distributed System

In a distributed-system deployment, RiskFort components are installed on different servers. This is done for security, performance, and/or to enable multiple applications to use the risk-evaluation functionality.

This deployment model is typically used for production deployments or for staging environments.

For example, the most common deployment is to install RiskFort Server on one system and one or more Web applications on additional systems. Because the deployment covers more than one system, an architecture diagram is included that indicates which systems must be able to communicate with each other.

To perform a distributed-system deployment you must select the **Custom** installation option (See "Installing on the First System" on page 5-74 for more information) option in the RiskFort installer.

The component diagrams and an architecture diagram for high-availability deployment are discussed in this section:

- Component Diagrams
- Architecture Diagram

Component Diagrams

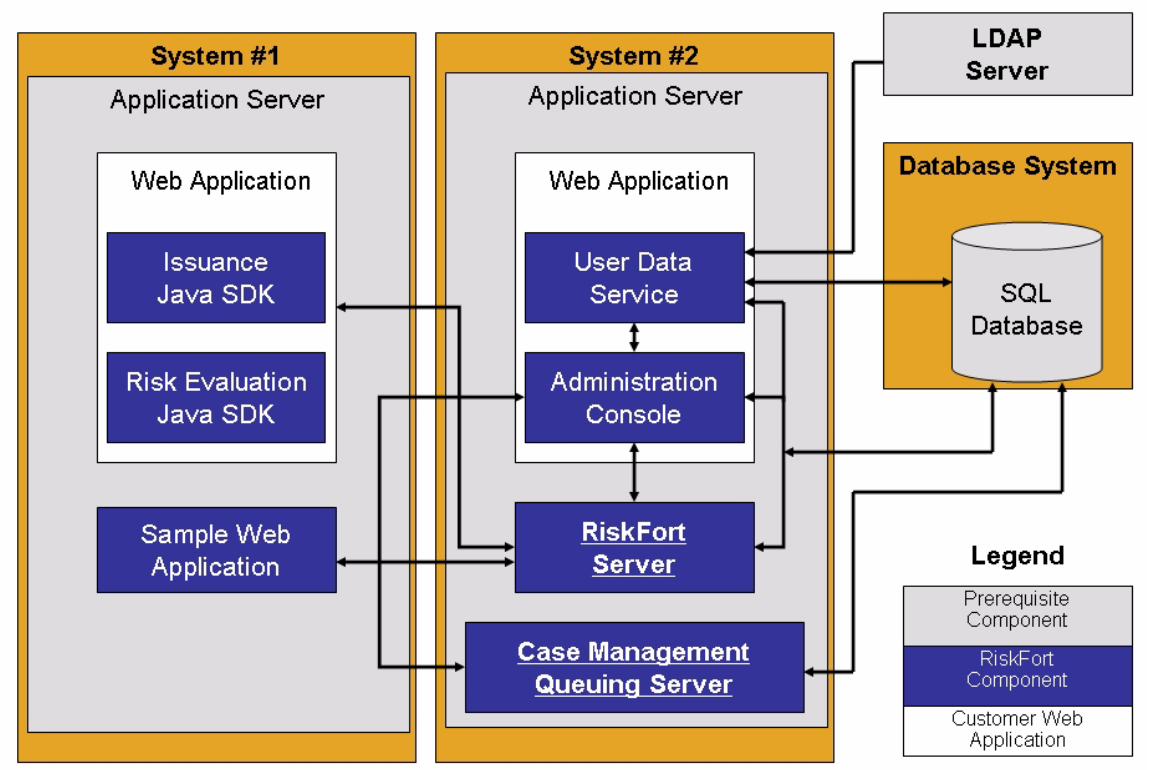
The diagrams in this section depict several possible options, where prerequisites and RiskFort components can be installed on multiple systems:

- Deploying Single Application with Java SDKs
- Deploying Multiple Applications with Java SDKs
- Deploying Single Application with Web Services

Deploying Single Application with Java SDKs

Figure 2-3 illustrates RiskFort using Java SDKs with a single application.

Figure 2-3 RiskFort (Java SDKs as Single Application) on Distributed Systems

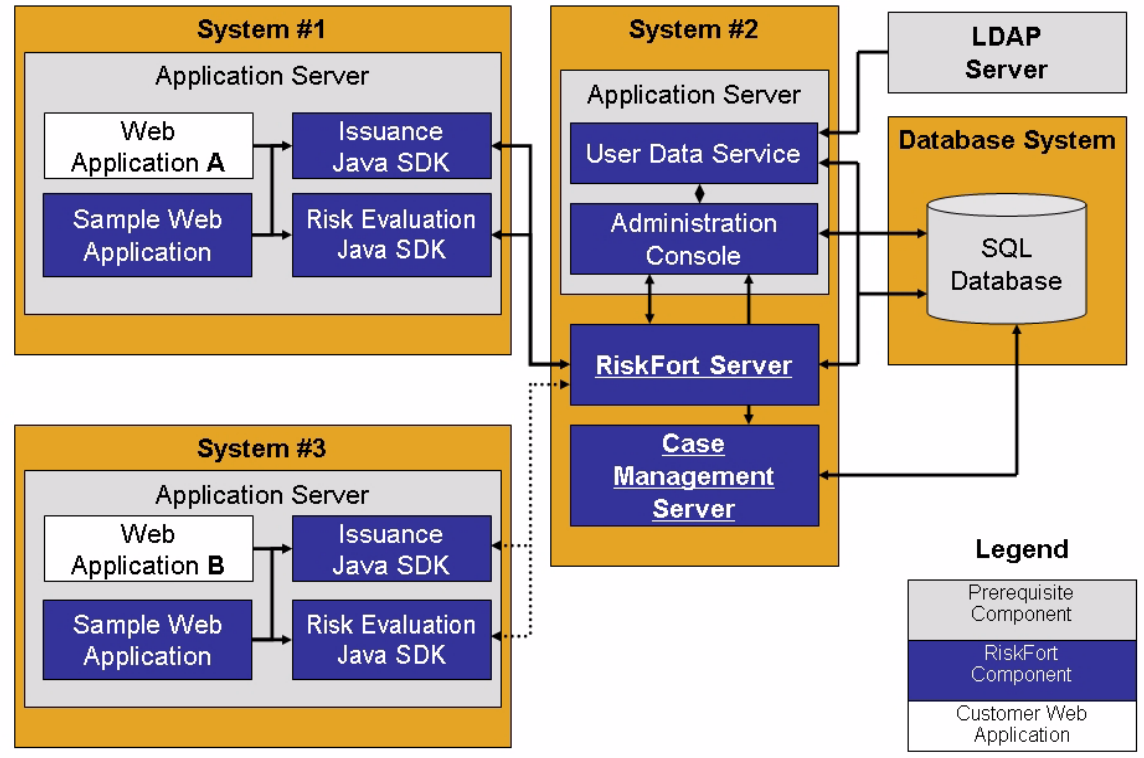


Note: The Administration Console can be installed on any individual system, every system, or on a system not listed in the diagrams.

Deploying Multiple Applications with Java SDKs

Figure 2-4 illustrates RiskFort deployment using Java SDK with multiple applications.

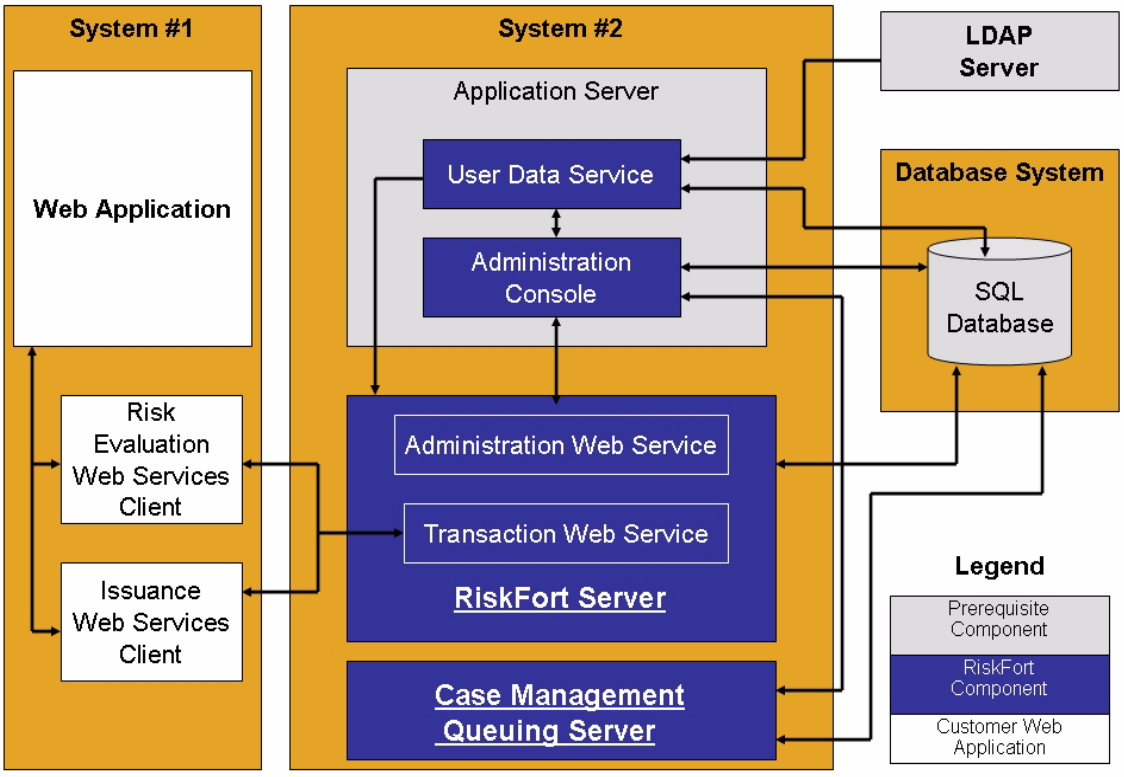
Figure 2-4 RiskFort (Java SDKs as Multiple Applications) on Distributed Systems



Deploying Single Application with Web Services

Figure 2-5 illustrates RiskFort deployment using Web Services on a single application.

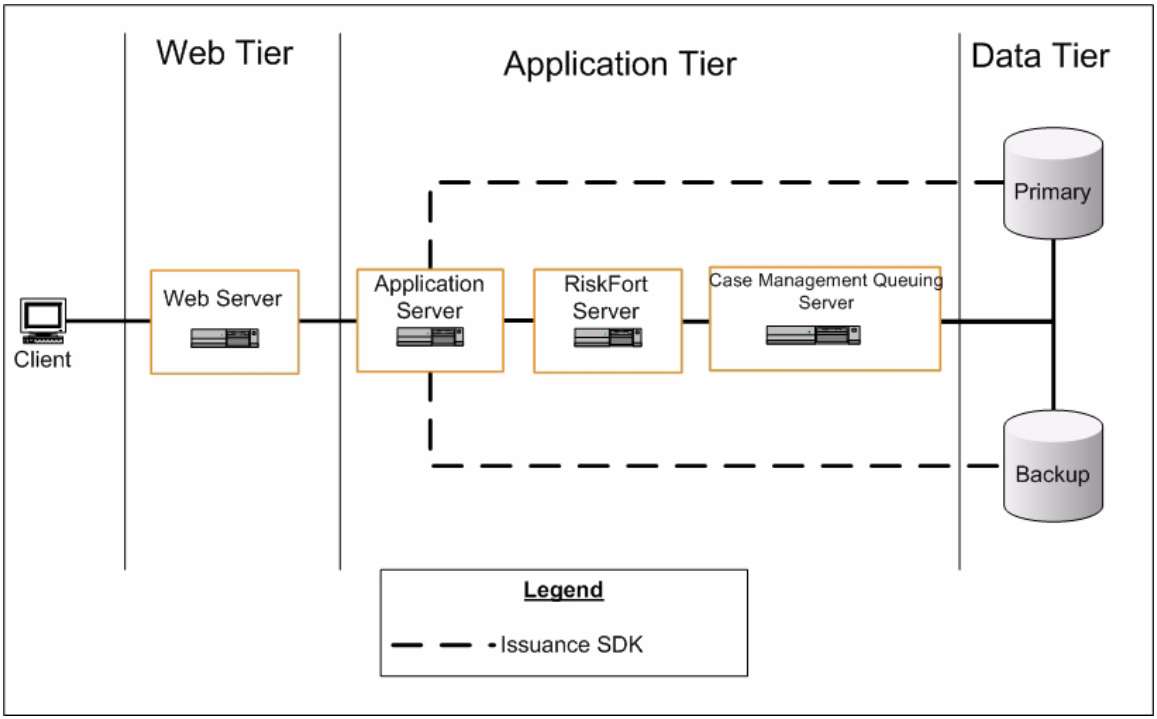
Figure 2-5 RiskFort (Web Services as Single Application) on Distributed Systems



Architecture Diagram

Figure 2-6 shows the architecture diagram for a distributed-system deployment.

Figure 2-6 Distributed Architecture Diagram



Note: Load balancers can be used where appropriate, based on your network architecture.

Decision:

Which RiskFort components will be installed on each system?

Deploying in High-Availability Environment

In a high-availability deployment, RiskFort components are installed on more than one servers to provide high availability and scalability.

This section discusses component diagrams and an architecture diagram for deploying in a high-availability environment:

- Component Diagrams
- High-Availability Architecture Diagram

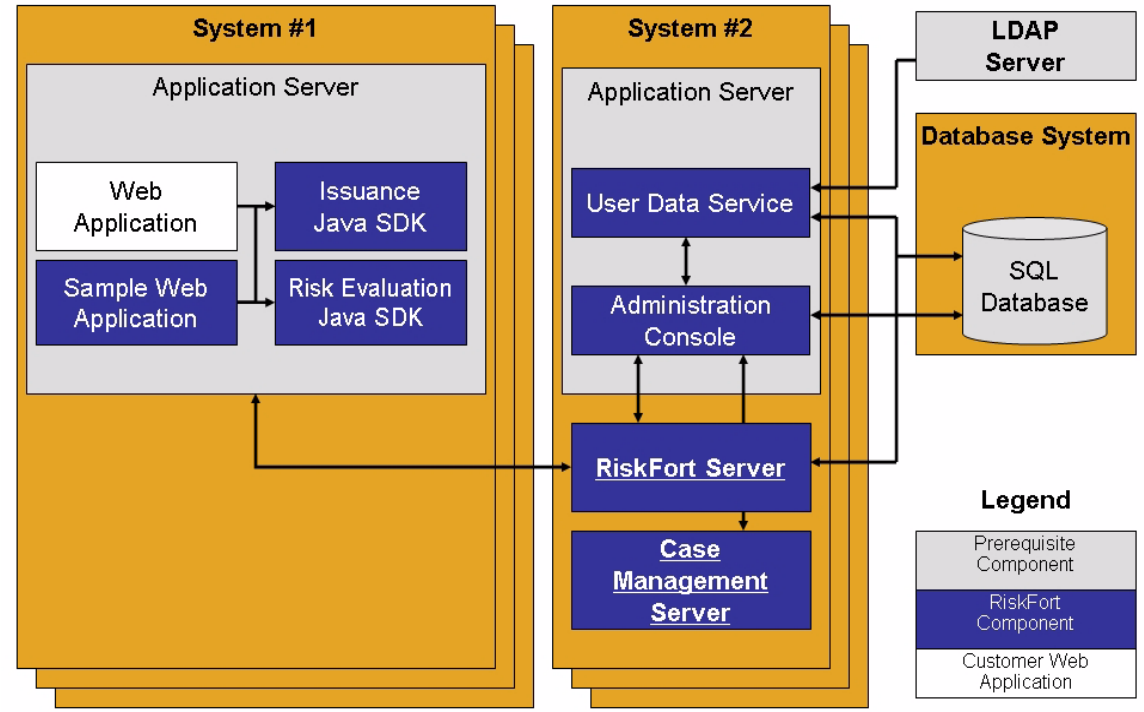
Component Diagrams

The diagrams in this section depict several possible options for which prerequisites and RiskFort components can be installed on multiple systems for a high-availability deployment.

High-Availability Deployment Using Java SDK

Figure 2-7 illustrates multiple-instance deployment of RiskFort using Java SDK.

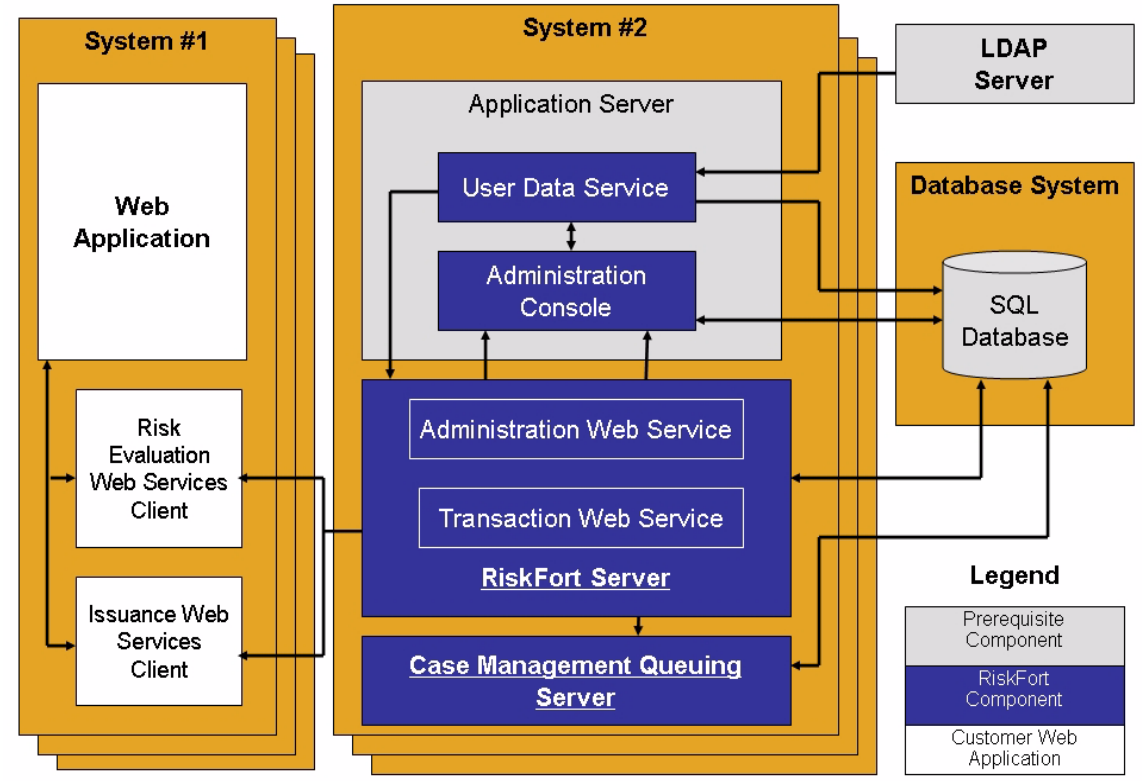
Figure 2-7 RiskFort (Java SDKs) in High-Availability Environment



High-Availability Deployment Using Web Services

Figure 2-8 illustrates multiple-instance deployment of RiskFort using Web Services.

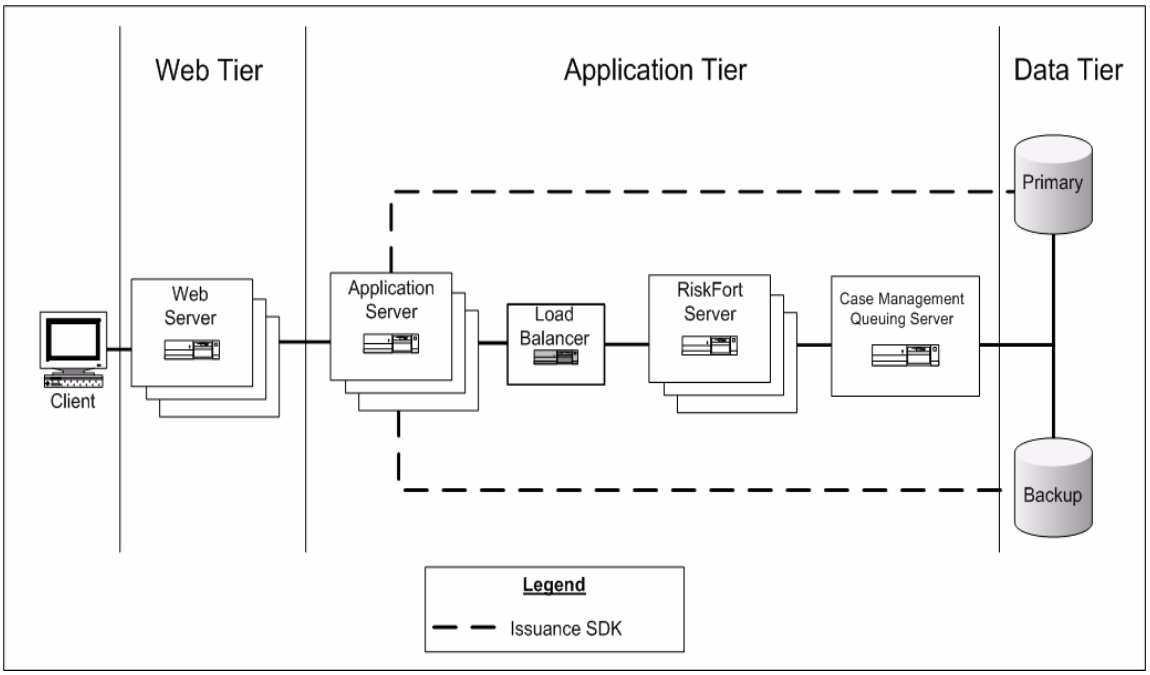
Figure 2-8 RiskFort (Web Services) in High-Availability Environment



High-Availability Architecture Diagram

Figure 2-9 shows the architecture diagram for a multiple-instance deployment.

Figure 2-9 High-Availability Architecture Diagram



Chapter 3
Preparing for Installation

Before installing RiskFort Server and its components, ensure that your computer meets the requirements described in this chapter. The chapter also provides configuration and planning-related information.

This chapter contains the following sections:

Hardware Requirements

The *minimum* hardware requirements for installing RiskFort include:

- Requirements for RiskFort with database on single system:
  - **RAM:** 2 GB
  - **Hard Drive Space:** 10 GB
  - **Processor:** 2.4 GHz
- Requirements for RiskFort with database on a different system:
  - **RAM:** 1 GB
  - **Hard Drive Space:** 300 MB

- **Processor:** 2.4 GHz

	**Note:** Resource requirements vary substantially for different applications and usage patterns. Arcot strongly recommends load-testing your site to determine the optimal memory required for the installation. While load-testing, you must keep in mind that some operating system utilities for monitoring memory can overstate memory usage (partially because of the representation of shared memory.) The preferred method for determining memory requirements is by monitoring the improvement in performance after adding more RAM/physical memory in the load test. Refer to your platform vendor documentation for information about how to configure memory and processor resources for testing purposes.

Software Requirements

The following information for software requirement is provided in this section:

- Minimum Software Requirements
- RiskFort Component-Specific Prerequisites

Minimum Software Requirements

Table 3-1 list of minimal software required to install RiskFort.

	**Note:** For all the third-party software mentioned in the Table 3-1, it is assumed that the higher versions are compatible with the specified supported version.

Table 3-1. Minimum Software Requirements

Software Type	Version
Operating System	Windows Server 2003 Enterprise Edition
Service Pack	SP2 or higher
Database Server	• **Server:** Microsoft SQL Server 2005, Standard Edition (SP2) or higher • **Client:** Microsoft SQL Server 2005 Client or compatible
	• **Server:** Oracle 10*g* or higher • **Client:** Oracle 10*g* or compatible

Table 3-1. Minimum Software Requirements

Software Type	Version
Directory Server	The following Directory Servers are supported: • Windows Active Directory 2003 • SunOne Directory Server 5.2 • SunOne Directory Server 6.1
Application Server	The following Application Servers are supported: • Apache Tomcat 5.5.23 or higher *(http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.23/bin/)* • IBM WebSphere 6.1 or higher • BEA WebLogic 10 or higher
JDK	The JDK version that is best compatible with the Application Server that you are using.

RiskFort Component-Specific Prerequisites

The prerequisite software is determined by the RiskFort components that will be installed on a system. Refer to Chapter 2, "Planning the Deployment" to determine which RiskFort components to install for each deployment type.

Table 3-2 indicates the prerequisite software required by each RiskFort component.

Table 3-2. Prerequisites for RiskFort Components

Component \ Prerequisite	Database Client	JDK	Application Server
RiskFort Server	✓		
Case Management Queuing Server	✓		
Administration Console		✓*	✓
Risk Evaluation Java SDK		✓*	✓
Issuance Java SDK		✓*	✓
Administration Web Service		✓*	✓
Transaction Web Service		✓*	✓
Sample Application		✓*	✓

* *The JDK depends on the application server you are using.*

Configuring Database Server

Before installing RiskFort, you must set up a database that is used for storing user information, server configuration data, audit log data, and other information.

RiskFort supports a primary database as well as a backup database that can be used during failover and failback in high-availability deployments. Database connectivity can either be configured as follows:

- During RiskFort installation
- By manually editing the arcotcommon.ini file.

There are specific configuration requirements for each supported database (Microsoft SQL Server or Oracle). Use the following information to set up the database server yourself, or provide this information to your database administrator (DBA) when you request a database account.

Important: To protect the database, Arcot strongly recommends that the database server is protected with firewall or other access control mechanisms and is set to the same time-zone as all Arcot products.

- Configuring Microsoft SQL Server
- Configuring Oracle Database

Configuring Microsoft SQL Server

This section provides the following configuration information for MS SQL Server:

Note: Refer to MS SQL Server documentation for detailed information on performing the tasks listed in this section.

1. Verifying Authentication Mode
2. Creating a Database
3. Creating a Database User

Verifying Authentication Mode

Verify that MS SQL Server is configured to use the "**SQL Server and Windows"** authentication method. RiskFort will not be able to connect to the database if SQL Server is configured to "**Windows Only**" authentication mode.

Creating a Database

Use the following criteria to create a database:

1. The recommended name is `arcotdb`.
2. The database size must be configured to automatically grow.

Creating a Database User

Use the following steps to create a database user:

Note: MS SQL Server refers to user as a `Login`.

1. Go to <***SQL_Server_Name***>, **Security**, **Logins** in the MS SQL Management GUI.
2. Enter the Login name. The recommended name is `arcotuser`.
3. Set the following parameters:
   a. Authentication to **SQL Server Authentication.**
   b. Default database to the database (`arcotdb`) created.
   c. Password for the login.
   d. User Mapping (SQL 2005) for the default database to `db_owner`.

Configuring Oracle Database

This section provides the configuration information for Oracle database and RiskFort Server.

Note: Refer to the Oracle database documentation for details on performing the tasks listed in the following sections.

Required Tablespaces

Running RiskFort on Oracle requires two tablespaces:

- The first tablespace is used for configuration data, audit logs, and user information. This tablespace can be the default user tablespace in the Arcot database.

  See "Creating a New Database" for creating a database.

- The second tablespace is used to run reports. For high performance, Arcot recommends that it be a separate tablespace.

Arcot Database Configuration Script

The Arcot database configuration script, `arcot-db-config-for-common-1.0.sql`, automatically creates the tablespace for reports if the database user running the script has sufficient permissions to create a tablespace. If the user does not have the required permissions, a DBA will need to manually create this tablespace and delete the section in this script which creates the reports tablespace.

Important: The parameters for creating the reports tablespace in the `arcot-db-config-for-common-1.0.sql` database script can be changed as per the DBA's preferences. However, the tablespace name must be `ARRFReports` to generate reports successfully.

Perform the following steps to setup the Oracle database:

1. Creating a New Database
2. Creating a Database User

Creating a New Database

Create a new database (recommended name is `arcotdb`) that stores information in the UTF-8 character set. This allows RiskFort to use international characters including double-byte languages.

Creating a Database User

Create a user with the following criteria:

1. Create a user (recommended name is `arcotuser`), with a schema in the new database `arcotdb`.

2. Set the quota of user to *at least* 5 to 10GB for a development or test deployment, which is primarily used for audit logs.

Note: If the deployment is for production, staging, or other intensive testing, refer to Appendix C, "Database Reference" to determine the quota required for an user.

3. Grant the user with `CONNECT` and `RESOURCE` privileges.
4. Grant the user with `CREATE TABLESPACE` privilege.
5. Grant the user with `CREATE TABLE` privilege.
6. Grant the user `ALTER EXTENT PARAMETERS` privilege.
7. Grant the user privileges to modify the storage extents for the LOB columns.

Getting Ready for Installation

Before you proceed with RiskFort installation, you must set up the RiskFort datastore, the Database Client, and gather the required Database information for use during the installation later. You must also ensure that the prerequisite JDK version and application server required by RiskFort components are installed.

This section discusses the following topics:

- Database Information that You Need for Installing RiskFort
- Requirements for Java-Dependent Components

Database Information that You Need for Installing RiskFort

Perform the tasks described in this section on the system where you will install RiskFort or the system that uses RiskFort components.

MS SQL Database

Get the following database information from the DBA. You will need this information when you install RiskFort:

1. **Server**
2. **Database**

3. **User Name**
4. **Password**

Refer to Step 7 on page 4-49 for more information on these parameters.

Oracle Database

Get the following database information from the DBA. You will need this information when you install RiskFort:

1. **Service ID** (Instance identifier of the Oracle database)
2. **Host Name**
3. **Port Number**
4. **User Name**
5. **Password**

Refer to Step 7 on page 4-49 for more information on these parameters.

Requirements for Java-Dependent Components

Install the following components required by Administration Console, RiskFort Java SDKs, and Web Services:

- **JDK**

Note: If you perform a fresh installation of JDK, then you *must* set the `JAVA_HOME` environment variable. The `path` variable must point to `%JAVA_HOME%\bin\`. If you fail to do so, then the Administration Console and other JDK-dependant components might fail to start.

- **Application Server**

Important: If you are performing a single-system deployment, where the Oracle Database Server and RiskFort components are installed on same system, then change the default port (`8080`) of Apache Tomcat. This avoids a conflict with the Oracle Database Server on port `8080`.

Pre-Installation Checklist

Arcot recommends that you complete this checklist before you proceed with the installation and setup of RiskFort.

Table 3-3. Pre-Installation Checklist

Your Information	Example Entry	Your Entry
HARDWARE		
Processor	Intel Xeon X5450 3 GHz	
RAM	2 GB	
Disk Space	20 GB	
SOFTWARE		
Operating System	Windows Server 2003	
Distribution	Enterprise Edition	
Service Pack (or Patch)	SP3	
DATABASE		
Type	Oracle	
DSN Name	arcotdsn	
Host Name (or Server)	arcotdsn	
Port (*Oracle Databases Only*)	1521	
Service ID (*Oracle Databases Only*)	oradb1	
User Name	rfdbadmin	
Password	password1234!	
Configured Privileges:		
CREATE TABLE	,	
CREATE INDEX	,	
CREATE PROCEDURE	,	
REFERENCES	,	
DML Privileges	,	
RESOURCE Privileges (*Oracle Databases Only*)	,	
CONNECT Privileges (*Oracle Databases Only*)	,	

Table 3-3. Pre-Installation Checklist

Your Information	Example Entry	Your Entry
ALTER EXTENT PARAMETERS (*Oracle Databases Only*)	,	
CREATE TABLESPACE (*Oracle Databases Only*)	,	
UNLIMITED TABLESPACE (*Oracle Databases Only*)	,	
DROP TABLESPACE (*Oracle Databases Only*)	,	
APPLICATION SERVER		
Type	Apache Tomcat 5.5	
Host Name	localhost	
Port	8080	
JDK	1.5.0_10	
DIRECTORY SERVICE		
Host Name	ds.myldap.com	
Port	389	
Schema Name	inetorgperson or user	
Base Distinguished Name	dc=myldap,dc=com	
User Name	cn=admin,cn=Administrators,cn=dscc	
Password	mypassword1234!	
WEB SERVER (OPTIONAL)		
Type	IIS 6	
Host Name	mywebserver.com	
Port	443	

Chapter 4
Deploying RiskFort On a Single System

Use the **Arcot RiskFort 2.2.6 InstallAnywhere Wizard** to install RiskFort components. This Wizard supports *Complete* and *Custom* installation types. However, to install and configure RiskFort on a single computer, you must use the **Complete** option when you run the installer.

The following steps provide a quick overview of the process:

1. Run the RiskFort installer to install RiskFort components and configure them to access your SQL database.

   See "Performing Complete Installation" for install instructions.

2. Execute the database scripts to create RiskFort schema and database tables. Also ensure that the database setup was successful.

   See "Creating a Data Source Name (DSN)", "Running Database Scripts" and "Verifying the Database Setup" for more information.

3. Deploy Web applications (UDS and Administration Console) on the application server and verify the deployments.

   See "Deploying Web Applications" for more information.

4. Log in to Administration Console with the Master Administrator credentials to initialize RiskFort.

   See "Logging in to Administration Console" and "Bootstrapping the System" for more information.

5. Start the RiskFort Server and Case Management Queuing Server and verify if the services start successfully.

   See "Starting RiskFort Server", "Starting the Case Management Queuing Server", and "Verifying the Installation" for more information.

6. (Optional) To ensure secure communication between RiskFort components, you can configure them to support SSL (Secure Socket Layer) transport mode.

   See Appendix F, "Configuring SSL" for more information.

7. Deploy and use Sample Application to test RiskFort configuration.

Note: Sample Application is automatically installed as a part of Complete installation.

See "Deploying Sample Application" and "Using Sample Application" for more information.

8. Complete the installation checklist.

See "Post-Installation Checklist" for more information.

Important Notes Related to the Installation

You must keep the following points in mind while installing RiskFort either on a single system or in a distributed environment:

- You must ensure that the `<install_location>` *must not contain* any special characters (such as `~ ! @ # $ % ^ & * ( ) _ + = { } [ ] ' "`).
- RiskFort 2.2.6 does not support upgrade from a previous version (1.7 or earlier). Also, you cannot install RiskFort 2.2.6 over a previously installed version.
- Currently, you cannot modify or repair RiskFort components by using the installer. You *must* uninstall the component and then re-install it.
- Do not close the installer window, if the installation is in progress. If at any time during installation (*especially during the last stages*), if you click the **Cancel** button to abort the installation, then the installer might not remove *all* the directories it has created so far. You will manually need to clean up the installation directory, `<install_location>\Arcot Systems\` and its subdirectories.

Performing Complete Installation

To install (and later configure) RiskFort on Windows successfully, the user account that you plan to use for installation *must* belong to the `Administrators` group. Else, some critical steps in the installation, such as DSN creation and configuration and RiskFort service creation, will not go through successfully, though the installation might complete without any errors.

Complete installation allows you to install all components of the RiskFort package. These components include RiskFort Server and the scripts required for setting up the Database that you intend to use for RiskFort.

Note: Before proceeding with the installation, ensure that all prerequisite software components are installed and the database is set up, as described in the Chapter 3, "Preparing for Installation".

Perform the following tasks to install RiskFort components:

1. Navigate to the directory where the `Arcot-RiskFort-2.2.6-Windows-Installer.exe` file is located and double-click the file to run the installation wizard.

   The Welcome screen appears.

2. Click **Next** to continue.

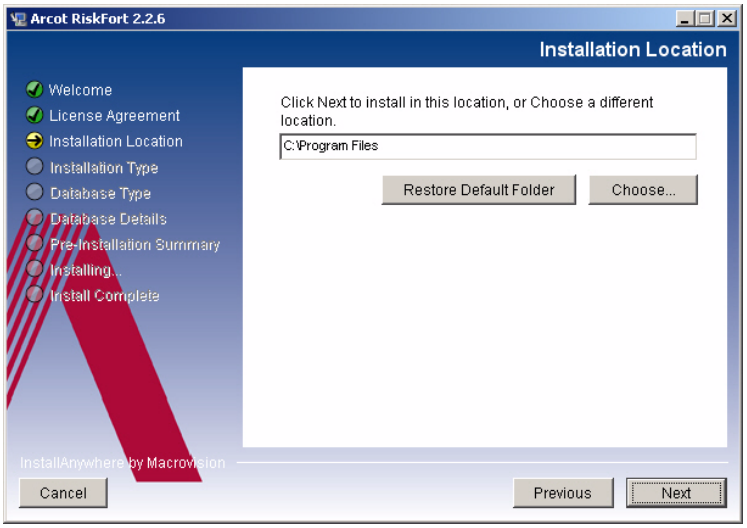
   The License Agreement screen appears.

3. Read the license agreement carefully, select the **I accept the terms of the License Agreement** option, and click **Next.**

   The installer now checks if any other Arcot product is installed on the computer.

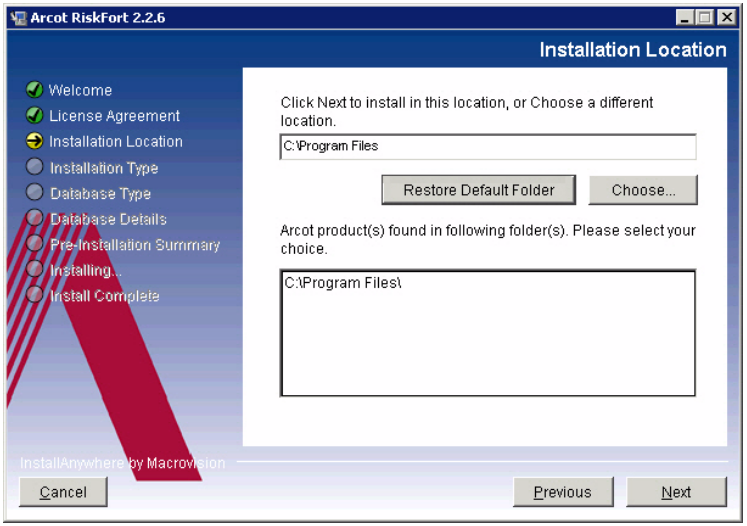
   If it does not find an existing Arcot product installation, then you will be prompted for an installation directory. In this case, the Installation Location screen, shown in the Figure 4-1 appears.

Figure 4-1 Installation Location Screen: No Installation Detected



If the installer detects an existing Arcot product installation, then you will not be prompted for an installation directory. The following screen (Figure 4-2) appears when an existing `ARCOT_HOME` was located on the computer.

Figure 4-2 Installation Location Screen: Previous Installation Detected



4. You can accept the default directory specified by the installer to install RiskFort. You can also click **Choose** to navigate and to specify a different directory.

   Click **Next** to install in the specified directory.

   The Installation Type screen appears.

5. Click **Complete** to install all components in one `ARCOT_HOME` and then click **Next** to continue.

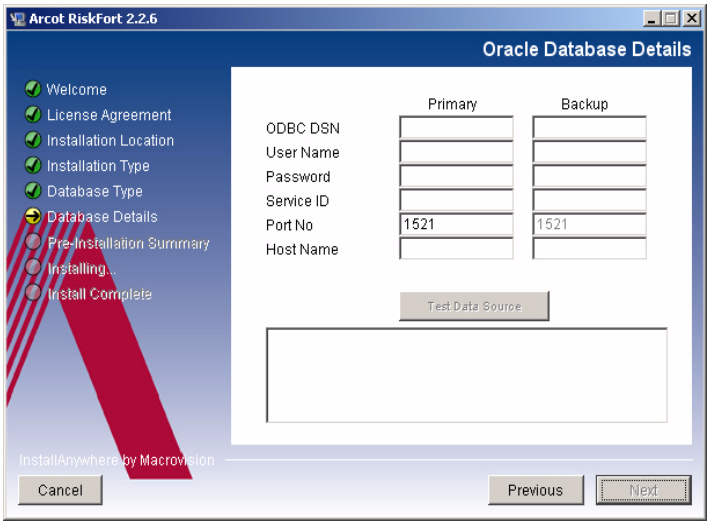
   The Database Type screen appears.

6. Depending on the type of database you have, you can either select **Oracle** or **Microsoft SQL Server**. Click **Next** to proceed.

   If you selected **Oracle** on the Database Type screen, then the Oracle Database Details screen (Figure 4-3) appears.

Database Source Name (DSN) specifies the information required to connect to a database by using an ODBC driver. This information includes database name, directory, database driver, User ID, and password.

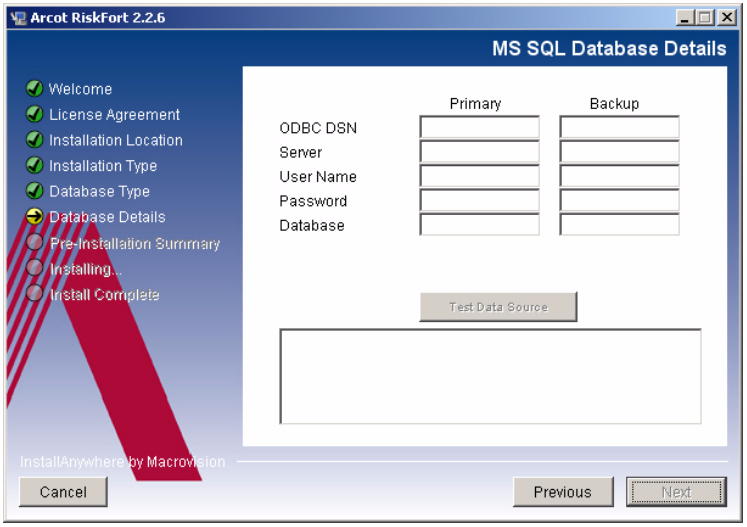
Figure 4-3 Oracle Database Details Screen



If you selected **Microsoft SQL** on the Database Type screen, then the MS SQL Database Details screen (Figure 4-4) appears. This screen slightly differs from the Oracle Database Details screen.

Note: If you are using MS SQL database, then you must ensure that the ODBC Driver version you are using is same as mentioned in the Chapter 3, "Preparing for Installation" section.

Figure 4-4 MS SQL Database Details Screen



7. **For Oracle** Primary and Backup databases, fill in the following information in the fields (Figure 4-3):

   - **ODBC DSN:** The name of the DSN, which refers to the RiskFort datastore. This value is used by the RiskFort Server to connect to the RiskFort datastore. The recommended value to enter is `arcotdsn`.
   - **User Name:** The database user name for RiskFort to access the database. This name is specified by the database administrator.

     This user *must* have the `create session` and DBA rights.

	**Note:** The **User Name** value for the Primary and Backup DSNs *must* be different.

   - **Password:** The password associated with the **User Name** you specified in the previous field and which is used by RiskFort to access the database. This password is specified by the database administrator.
   - **Service ID:** The Oracle System Identifier (SID) that refers to the instance of the Oracle database running on the server.

- **Port:** The port at which the specified database listens to incoming requests. The default port at which an Oracle database listens is `1521`. However, if you would like to specify another port, enter the port value in this field.
- **Host Name:** The host name or IP address of the RiskFort datastore.

  Syntax: `<server_name>`

  Example: `demodatabase`

For MS SQL Primary and Backup databases, fill in the following information in the fields (Figure 4-4)

- **ODBC DSN:** The name of the DSN, which refers to the RiskFort datastore. This value is used by the RiskFort Server to connect to the RiskFort datastore. The recommended value to enter is `arcotdsn`.
- **Server:** The host name or IP address of the RiskFort datastore.
  - **Default Instance**

    Syntax: `<server_name>`

    Example: `demodatabase`
  - **Named Instance**

    Syntax: `<server_name>\<instance_name>`

    Example: `demodatabase\instance1`
- **User Name:** The database user name for RiskFort Server to access the datastore. This name is specified by the database administrator. (MS SQL Server, typically, refers to this as `login`.)

  This user *must* have the `create session` and DBA rights.

  Important: The **User Name** value for the Primary and Backup DSNs *must* be different.

- **Password:** The password associated with the **User Name** you specified in the previous field and which is used by RiskFort to access the datastore. This password is specified by the database administrator.
- **Database:** The name of the MS SQL database instance.

8. Click **Next** to continue.

The Pre-Installation Summary screen appears.

Review the information on this screen, and if you need to change a previous selection, then click **Previous** to do so. After changing the required selection, click **Next** to go to the next screen.

9. Click **Install** to begin the installation process.

   The Installing Arcot RiskFort screen appears. This might take several minutes. After some time the Installation Complete screen appears.

10. Click **Yes** to restart the computer.

    RiskFort Server launches correctly only *after* the computer has been restarted.

11. Click **Done** to complete the RiskFort Server installation.

Note: After the installation is completed, perform the post-installation tasks discussed in "Performing Post-Installation Tasks".

Installation Logs

After installation, you can access the installation log file (`Arcot_RiskFort_InstallLog.log`) at the following directory:

`<install_location>\Arcot Systems\logs\`

If for some reason, the installation failed, then the error log is available in the same location where you ran the Installer from.

Performing Post-Installation Tasks

This section guides you through the post-installation tasks that you must perform after installing RiskFort. These steps are required for configuring RiskFort correctly and must be *performed in the following order*:

1. Creating a Data Source Name (DSN)
2. Running Database Scripts
3. Verifying the Database Setup
4. Deploying Web Applications
5. Logging in to Administration Console

6. Bootstrapping the System
7. Starting RiskFort Server
8. Starting the Case Management Queuing Server
9. Verifying the Installation
10. Deploying Sample Application
11. Using Sample Application

Note: After completing these post-installation tasks, perform the SDK and Web Services configuration tasks discussed in Chapter 6, "Configuring RiskFort SDKs and Web Services".

Creating a Data Source Name (DSN)

To create the DSN for your Microsoft SQL Server or the Oracle Database Server:

1. Open the Control Panel, navigate to **Administrative Tools, Data Sources (ODBC), System DSN**, and click **Add**.
2. Select the required DSN type, and click **Finish**.
3. Create the DSN for the database by using the details provided in Step 7 on page 4-49.
4. Click **OK** to create the DSN.

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

Running Database Scripts

Important: Before you run the scripts discussed in this section, you must ensure that you are logged in as the same database user that you created in the "Configuring Database Server" in Chapter 3 section.

RiskFort is shipped with scripts that are required to create necessary tables in the RiskFort database. To run the required database scripts:

1. Navigate to the following directory:

   `<install_location>\Arcot Systems\dbscripts\`

2. Based on the database you are using, navigate to one of the following folders:

- **For Oracle:**

  `<install_location>\Arcot Systems\dbscripts\oracle\`

- **For MS SQL:**

  `<install_location>\Arcot Systems\dbscripts\mssql\`

3. Run the scripts *in the following order*:
   - `arcot-db-config-for-common-1.0.sql`
   - `arcot-db-config-for-riskfort-2.2.6.sql`

Verifying the Database Setup

After running the required database scripts, you must verify whether the RiskFort schemas were seeded correctly. To do so:

1. Log in to the RiskFort database as a user with `SYSDBA` privileges.
2. Run the following query:

   ```
   SELECT SERVERNAME, VERSION FROM ARRFSERVERS;
   ```

   You must see the following output as a result of the preceding query:

   ```
   SERVERNAME                    VERSION
   ------------------------  ----------------
   RiskFort                       2.2.6
   RiskFortCaseManagement         2.2.6
   ```

3. Log out of the database console.

Deploying Web Applications

Two components of RiskFort, User Data Service (UDS) and Administration Console, are Web-based and can be deployed on any of the following supported application servers:

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Before you deploy the WAR files for these Web applications on the application server of your choice, you must copy the Arcot-proprietary files required by UDS and Administration Console to the appropriate location on your application server. This section walks you through the steps to copy the required crypto-files to your application server and to deploy the WAR files of these Web applications:

1. Preparing Your Application Server
2. (Optional) Creating Enterprise Archive Files
3. Deploying User Data Service (UDS)
4. Verifying UDS Deployment
5. Deploying Administration Console
6. Verifying Administration Console Deployment

Preparing Your Application Server

UDS and Administration Console use the following files to access the RiskFort database securely:

- `arcot-crypto-util.jar` available at:

  `<install_location>\Arcot Systems\java\ext\`
- `ArcotAccessKeyProvider.dll` available at:

  `<install_location>\Arcot Systems\java\ext\win\<32\or\64\bit>\`

As a result, these files must be copied to the appropriate location on the application server where you have deployed these RiskFort components. The following subsections provide information on copying these files for:

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Apache Tomcat

To copy the Arcot-proprietary files:

1. Copy `arcot-crypto-util.jar` *to* `%JAVA_HOME%\jre\lib\ext\`.
2. Copy `ArcotAccessKeyProvider.dll` *to:* `%JAVA_HOME%\jre\bin\`.
3. Restart the application server.

IBM WebSphere

To copy the Arcot-proprietary files:

1. Log into WebSphere Administration Console.
2. Click **Environment,** and then click **Shared Libraries**.
   a. From the **Scope** drop-down, select a valid visibility scope. The scope must include the target server or node on which the application is deployed.
   b. Click **New**.
   c. Enter the **Name**, for example, *ArcotJNI*.
   d. Specify the **Classpath**.

      This path must point to the location where the `arcot-crypto-util.jar` file is present and must also include the file name. For example, `C:\Program Files\Arcot Systems\ext\`**`arcot-crypto-util.jar`**.
   e. Enter the JNI Library path.

      This path must point to the location where the `ArcotAccessKeyProvider.dll` file is present.
3. Click **Apply** to save the changes.
4. Configure the server-level class loaders.
   a. Click **Servers**, and then click **Application Servers.**
   b. Under **Application Servers** access the settings page of the server for which the configuration are performed.
   c. Click **Java and Process Management** and then click **Class Loader**.
   d. Click **New**.
   e. Select default **Classes loaded with parent class loader first** and click **OK.**
   f. Click the auto-generated **Class Loader ID**.
   g. On the class loader **Configuration** page, click **Shared Library References**.
   h. Click **Add**, select **ArcotJNI,** and then click **Apply**.
   i. Save the changes made.
5. Copy `ArcotAccessKeyProvider.dll` to `<`*`WebSphere_JAVA_HOME`*`>\jre\`**`bin`**`\`.
6. Restart WebSphere.

BEA WebLogic

To copy the Arcot-proprietary files:

1. Copy `ArcotAccessKeyProvider.dll` to WebLogic's `<WebLogic_JAVA_HOME>\jre\bin\`.
2. Copy `arcot-crypto-util.jar` to WebLogic's `<WebLogic_JAVA_HOME>\jre\lib\ext\`.

Note: Ensure that you use the appropriate `<JAVA_HOME>` used by WebLogic.

3. Login to WebLogic Administration Console.
4. Navigate to **Deployments**.
5. Enable the **Lock and Edit** option.
6. Click **Install** and navigate to the directory that contains the `arcot-crypto-util.jar` file.
7. Click **Next** to open the Application Installation Assistant.
8. Click **Next** to display the Summary page.
9. Click **Finish**.
10. Activate the changes.
11. Restart the server.

(Optional) Creating Enterprise Archive Files

By default, Arcot provides Web ARchive (WAR) files to deploy UDS and Administration Console. However if required, you can also change the format of these files to Enterprise ARchive (EAR) and then deploy the EAR files.

As discussed in the following subsections, you can either generate separate EAR files for both UDS and Administration Console, or you can generate a single EAR file that contains both Web archives.

Generating Separate EAR Files

To create separate EAR files for UDS and Administration Console:

1. Open the Command Prompt window.

2. Navigate to the `<install_location>\Arcot Systems\tools\bundlemanager\` directory.
3. Run the following command to create the EAR file:

   ```
   java -jar bundle-manager.jar -ear <filename.ear> -warList
   <filename.war>
   ```

   The preceding command generates individual EAR files that are available at:

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

Generating a Single EAR File

To create a single EAR file that contains the UDS and Administration Console Web archives:

1. Open the Command Prompt window.
2. Navigate to the `<install_location>\Arcot Systems\tools\bundlemanager\` directory.
3. Run the following command to create the EAR file:

   ```
   java -jar bundle-manager.jar -ear <filename.ear> -warList
   arcotadmin.war arcotuds.war
   ```

   The preceding command generates a single EAR file that is available at:

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

Deploying User Data Service (UDS)

User Data Service (UDS) enables access to the third-party data repositories (LDAP directory servers) deployed by your organization. As a result, it enables RiskFort Server and the Administration Console to seamlessly access your existing data. If the LDAP directory server is not configured, then it accesses the RiskFort database to read the user information. (See Step 3 on page 4-64 in the bootstrapping steps to know about the parameters that must be set to connect UDS to other RiskFort components.)

You need the `arcotuds.war` file to deploy User Data Service (UDS). To deploy UDS by using this file:

1. Deploy `arcotuds.war` on the application server. This file is available at:

Note: The deployment procedure depends on the application server that you are using. Refer to your application server vendor documentation for detailed instructions.
For example, in case of Apache Tomcat, you must deploy the WAR file at `<APP_SERVER_HOME>\webapps\`.

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

2. (**For WebSphere Only**) Configure to reload the UDS class when the application files are updated.
   a. Navigate to **Application**, **Enterprise Applications** and access the UDS settings page.
   b. Under **Class loader order**, select the **Classes loaded with local class loader first (parent last)** option.
   c. Under **WAR class loader policy**, select the **Single class loader for application**.
   d. Click **Apply** to save the changes.
3. Restart the application server.

Verifying UDS Deployment

The `arcotuds.log` file is used for logging UDS-related information. To verify if UDS started correctly:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotuds.log` file in any editor and locate the following lines:
   - `Initializing Arcot User Data Service (Version: 1.0.9)`
   - `Arcot User Data Service initialized successfully.`

   These lines indicate that UDS was deployed successfully.

Note: You might also want to make sure that the log files *do not* contain any `FATAL` *and* `WARNING` messages.

Deploying Administration Console

The *Administration Console* is a browser-based interface to RiskFort that enables you to customize the server configurations and manage the deployed system.

Note: To manage RiskFort by using Administration Console, you must ensure that Administration Console can access the system where the RiskFort Server is installed by its `hostname`.

You need the `arcotadmin.war` file to deploy the RiskFort Administration Console. This file is available at:

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

To deploy the Administration Console WAR file on your application server:

1. Deploy `arcotadmin.war` in the appropriate directory on the application server.

Note: The deployment procedure depends on the application server that you are using. Refer to your application server vendor documentation for detailed instructions.
For example, in case of Apache Tomcat, you must deploy the WAR file at `<APP_SERVER_HOME>\webapps\`.

2. Restart the application server.

Verifying Administration Console Deployment

The `arcotadmin.log` file is used for logging the Administration Console information.

To verify if the Administration Console was deployed successfully:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotadmin.log` file in any editor and locate the following lines:
   - `Arcot Administration Console v1.0.9`
   - `Arcot Administration Console Configured Successfully.`

These lines indicate that your Administration Console was deployed successfully.

Note: You might also want to make sure that the log files *do not* contain any `FATAL` *and* `WARNING` messages.

Logging in to Administration Console

When logging in to the Administration Console for the first time, you *must* use the **Master Administrator** (MA) credentials that are configured automatically in the database during the deployment.

To log in to the Administration Console as MA:

1. Start the Administration Console in a Web browser window. The default URL for the Administration Console is:

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

   Note: The host and port information that you specify in the preceding URL must be of the application server where you deployed the Administration Console.

2. Log in by using the default Master Administrator account credentials. The credentials are:
   - **User Name: masteradmin**
   - **Password: master1234!**

Important: Arcot strongly recommends that you change the Master Administrator password after the first log in.
Refer to the *Arcot RiskFort Administration Guide* for more information on changing the administrator password.

Bootstrapping the System

Before you can start using the Administration Console to manage RiskFort, you must first perform the following mandatory steps to initialize the system:

- Change the default Master Administrator password
- Set up UDS connectivity parameters

- Specify the authentication mechanism for the Default organization

Bootstrapping is a Wizard-driven process that walks you through these setup tasks. Other administrative links are enabled only after you perform these tasks.

Before you proceed with "Performing the Bootstrapping Tasks", you must understand the related concept of "Default Organization".

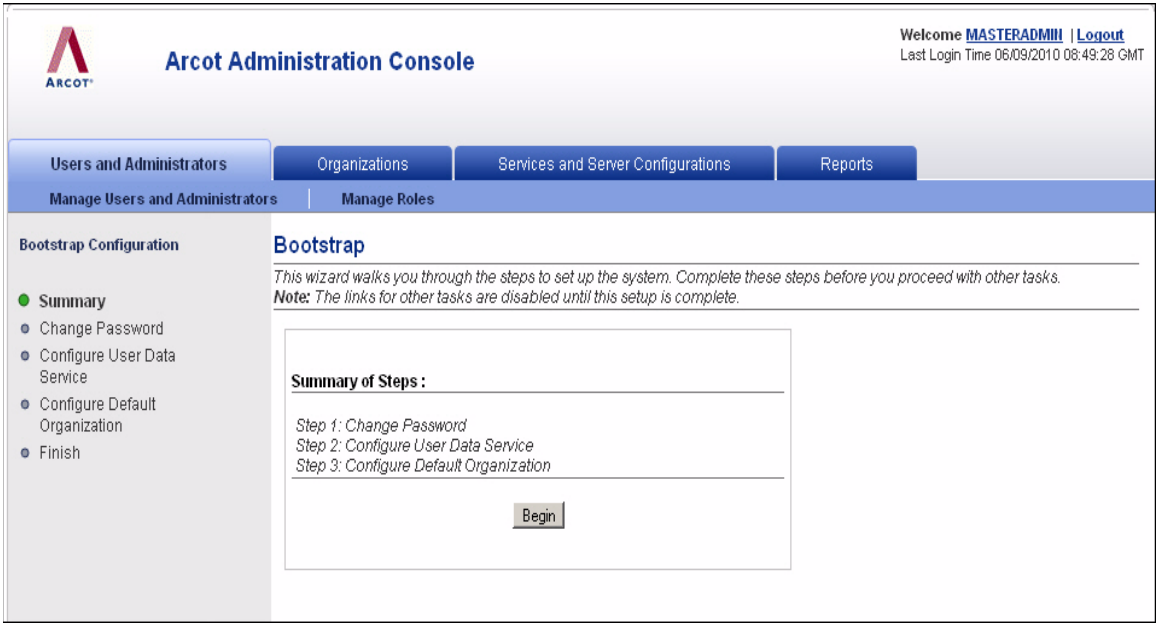
Default Organization

When you deploy the Administration Console, an organization is created automatically. This organization is referred to as *Default Organization* (`DEFAULTORG`). As a single-organization system, the Default Organization itself can be used without creating any new organizations.

Performing the Bootstrapping Tasks

When you first log in to the Administration Console as the Master Administrator (MA), the Summary screen for the Bootstrap wizard screen (Figure 4-5) appears.

Figure 4-5 Bootstrap Wizard: Summary Screen

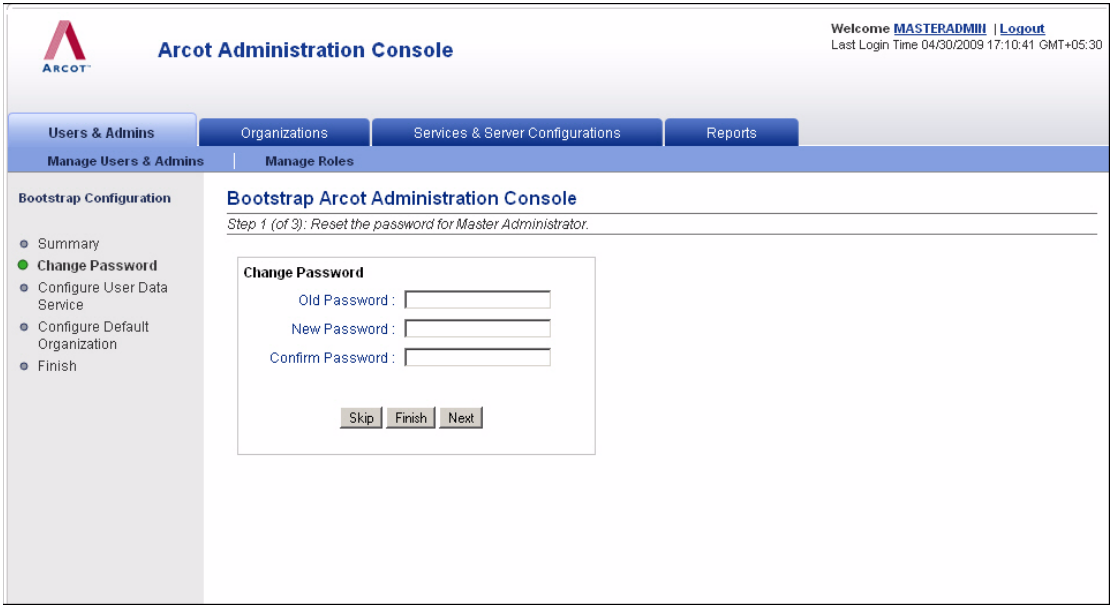


To bootstrap the system using the wizard:

1. Click **Begin** to start the process.

   The Change Password screen, as shown in Figure 4-6, appears.

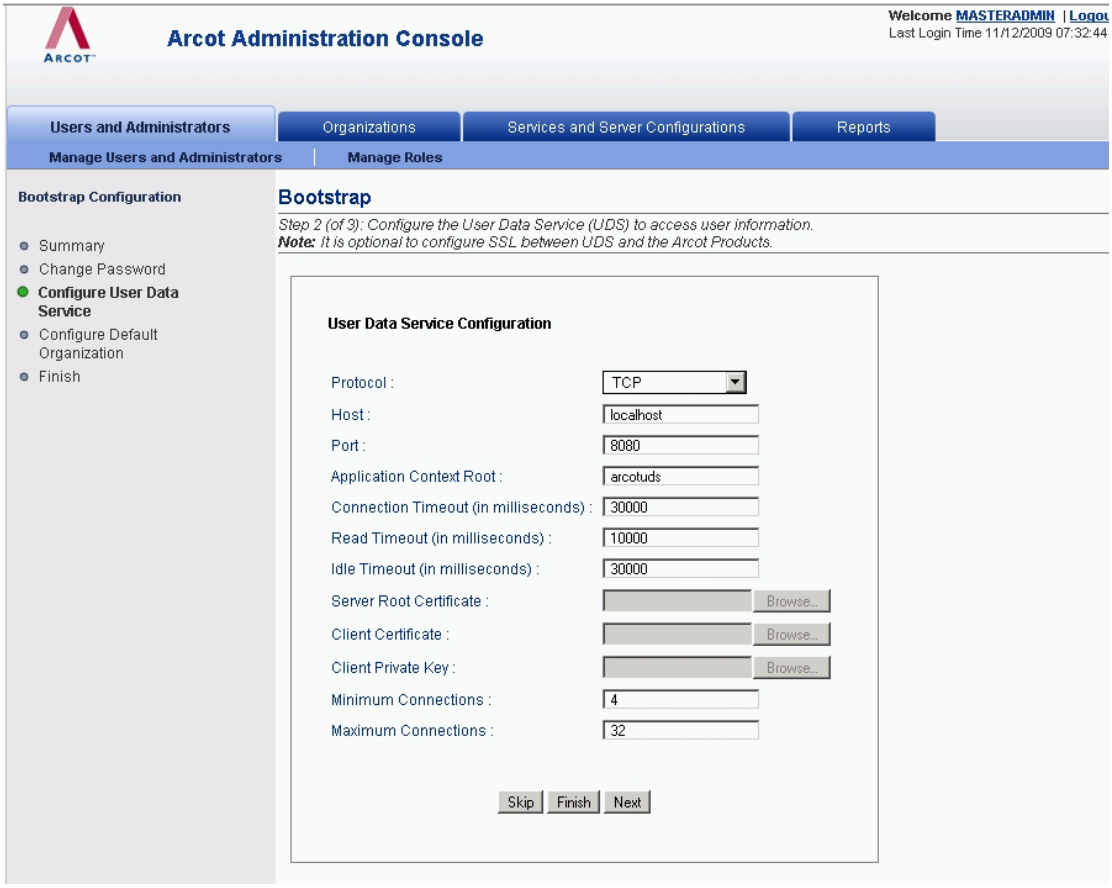
Figure 4-6 Bootstrap Wizard: Change Password Screen



2. Specify the **Old Password**, **New Password**, **Confirm Password**, and click **Next.**

   The Configure User Data Service screen, as shown in Figure 4-7, appears.

Figure 4-7 Bootstrap Wizard: Configure User Data Service Screen



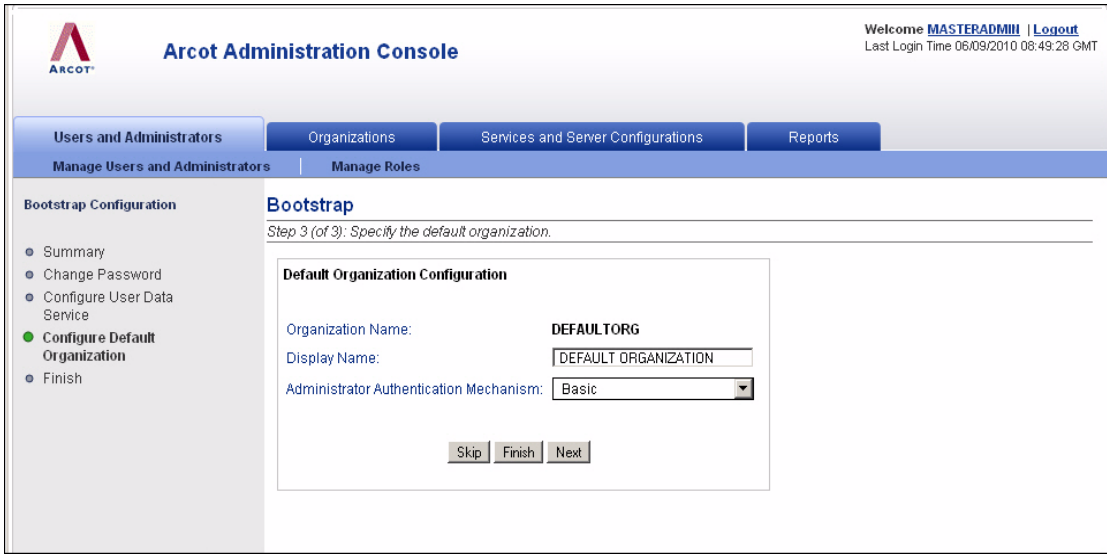
3. Specify the parameters listed in Table 4-1 to configure UDS:

Table 4-1. UDS Configuration Parameters

Parameter	Default Value	Description
Protocol	TCP	The protocol to connect to the UDS using the Administration Console. The available options are: • `TCP` • `One way SSL` • `Two way SSL`
Host	localhost	The host name or the IP address of the application server where the UDS is deployed.
Port	8080	The port on which the application server is available.
Application Context Root	arcotuds	The tag that is used to define UDS in the application server. For example, the context root in the *http://<host>:<port>/arcotuds/services* URL is `arcotuds`.
Connection Timeout (in milliseconds)	30000	Maximum time in **milliseconds** before the UDS service is considered unreachable.
Read Timeout (in milliseconds)	10000	Maximum time in **milliseconds** to wait for a response from UDS.
Idle Timeout (in milliseconds)	30000	Maximum time in **milliseconds** after which an idle connection will be closed.
Server Root Certificate	No Default	Upload the CA certificate file of UDS server. The file must be in PEM format.
Client Root Certificate	No Default	Upload the CA certificate file of the RiskFort Server. The file must be in PEM format.
Client Private Key	No Default	The location of file that contains the CA's private key.
Minimum Connections	4	The minimum number of connections that will be created between the RiskFort Server and UDS.
Maximum Connections	32	The maximum number of connections that can be created between the RiskFort Server and UDS.

The Configure Default Organization screen, shown in Figure 4-8, appears.

Figure 4-8 Bootstrap Wizard: Configure Default Organization Screen



4. Specify the following parameters for the Default Organization:

- **Display Name:** The descriptive name of the organization. This name appears on all other Administration Console pages and reports.
- **Authentication Mechanism:** The mechanism that is used to authenticate administrators belonging to the Default Organization. Administration Console supports two types of authentication methods for the administrators to log in:
  - **Basic User Password**

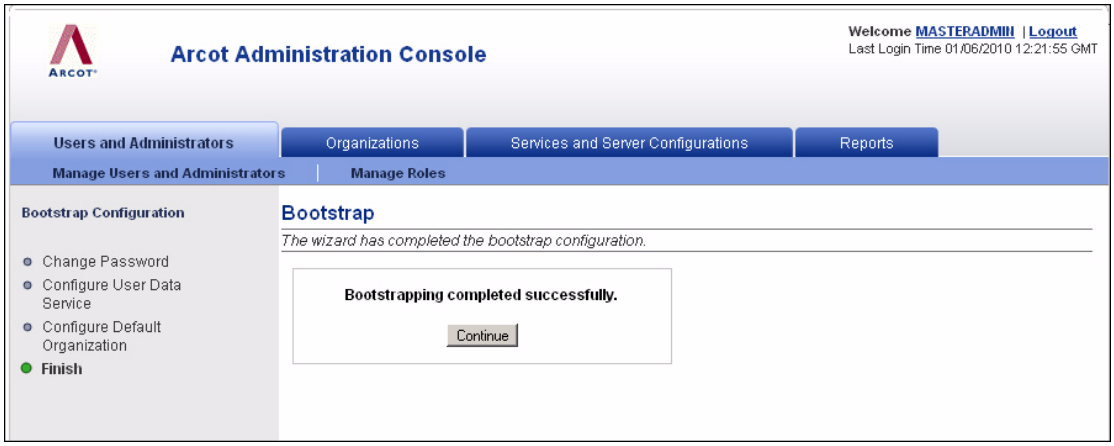
    If you choose this option, then the built-in authentication method provided by the Administration Console is used for authenticating the administrators.
  - **WebFort User Password**

    If you select the **WebFort User Password** option here, then the credentials are issued and authenticated by the WebFort Server. For this, the Arcot WebFort Server must be installed.

	Book: See the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on installing and configuring WebFort.

The Administration Console initialization is completed, as indicated in the Finish screen (Figure 4-9).

Figure 4-9 Bootstrap Wizard: Finish Screen



5. Click **Continue** to proceed with other configurations using the Administration Console.

Starting RiskFort Server

To start the RiskFort Server:

1. Click the **Start** button on your desktop window.
2. Navigate to **Settings, Control Panel, Administrative Tools,** and then **Services.**
3. Locate and double-click **Arcot RiskFort Service**.
4. Click **Start** in the service's window.

Note: If you want to stop the RiskFort Server, then follow the Steps 1 through 3, and click the **Stop** button in the service's window.

Starting the Case Management Queuing Server

To **start** the Case Management Queuing Server:

1. Click the **Start** button on your desktop window.
2. Navigate to **Settings, Control Panel, Administrative Tools,** and then **Services.**

3. Locate and double-click the **Arcot RiskFort Case Management Queuing Service**.
4. Click **Start** in the service's window.

Note: If you want to stop the Case Management Queuing Server, then follow the Steps 1 through 3, and click the **Stop** button in the service's window.

To **verify** if the Case Management service started successfully:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotriskfortcasemgmtserver.log` file in any editor and locate the following lines:

   - `STARTING Arcot RiskFort Case Management 2.2.6_w`
   - `Arcot RiskFort Case Management Service READY`

Note: You might also want to make sure that the log file does not contain any `FATAL` and `WARNING` messages.

Verifying the Installation

After you have seeded the database schema, deployed UDS and Administration Console, and bootstrapped the system, and started the Server, you must ensure whether all these components have started correctly. The log files that you need to verify for this purpose is `arcotriskfort.log`.

To verify if the server started correctly:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotriskfort.log` file in any editor and locate the following lines:

   - `STARTING Arcot RiskFort 2.2.6_w`

- `Arcot RiskFort Service READY`

Note: You might also want to make sure that the log file does not contain any `FATAL` and `WARNING` messages.

Deploying Sample Application

Important: Sample Application *must* be deployed on the same application server where Risk Evaluation and Issuance SDKs are Installed.

Sample Application can be used to verify if RiskFort was installed and configured properly. In addition, it demonstrates:

- The typical RiskFort workflows
- Basic operations (invocation and post-processing) of RiskFort APIs
- Integration of your application with RiskFort

Sample Application is automatically installed as a part of Complete installation of RiskFort. To deploy the Sample Application:

1. Navigate to **Settings, Control Panel, Administrative Tools,** and the select **Services.**
2. Stop the application server services.
3. Deploy the `riskfort-2.2.6-sample-application.war` file from `the following location:`

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

   Note: Although you will also see `riskfort-2.2.6-sample-application.war` in the package, it is recommended that you deploy the Sample Application file from the preceding location.

4. Navigate to **Settings, Control Panel, Administrative Tools,** and then select **Services.**
5. Restart the application server.

Using Sample Application

This sub-section describes the risk-evaluation operations that can be performed using Sample Application. Each operation in the sample application is designed to run without error when RiskFort is completely installed and functional.

Sample Application demonstrates the following operations that RiskFort Issuance and RiskFort Server can perform:

- Performing Risk Evaluation and Post Evaluation for a First-Time User
- Creating Users
- Performing Risk Evaluation and Post Evaluation for a Known User
- Editing the Default Profile and Performing Risk Evaluation

Performing Risk Evaluation and Post Evaluation for a First-Time User

To perform risk evaluation on the default profile of a user:

1. Ensure that Sample Application is open (in a Web browser window.) The default URL for Sample Application is:

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp

2. Click **Evaluate Risk** to open the Risk Evaluation page.
3. On the page, specify the name of the user (who you want to evaluate) in the **User Name** field.
4. Specify the name of the organization to which the user belongs in the **User Organization** field.
5. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score, the associated Risk Advice, and lists the rules that are configured for the specified organization. For a first-time user, the result is **ALERT**.

6. Click **Next Step** to open the Post Evaluation page and perform post-evaluation on the specified user profile.

   By using Post evaluation, your application provides feedback to RiskFort Server about the current user and/or the device they are using. RiskFort updates user and/or device attributes and the user-device association based on this feedback, and accordingly assesses risk associated with the transactions for the user in future.

7. Specify the result of secondary authentication by selecting the appropriate option from the **Result of Secondary Authentication** list.

8. Specify the name for the user name-device association in the **Association Name** field.
9. Click **Post Evaluate** to complete the post evaluation process and to display the result of the same in the Post Evaluation Results section.

Creating Users

To create a user:

1. Start the Sample Application in a Web browser window. The default URL for Sample Application is:

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp

   The RiskFort Sample Application page appears.
2. Click **Create User** to open the Create User page.
3. Enter a unique user name and their organization name in the **User Name** and **Organization Name** fields, respectively and click **Create User.** If you do not specify the **Organization Name**, then the user is created in `defaultorg`.

   The "The User is created successfully" message appears if the specified user was successfully added to the database.
4. Click **Main Page** to return to the RiskFort Sample Application page.

Performing Risk Evaluation and Post Evaluation for a Known User

1. On the Main Page of the Sample Application, click **Evaluate Risk** to open the Risk Evaluation page.
2. Specify the name of the user you created in the **User Name** field.
3. Specify the user's organization in the **User Organization** field.
4. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   The Risk Advice typically is **INCREASEAUTH**.
5. Click **Next Step** to perform Post Evaluation:
   - Specify the **Result of Secondary Authentication** from the list.
   - Edit the **Association Name**, if required.
6. Click **Post Evaluate** to display the final advice.

   If you repeat Step 1 through Step 4, the **Risk Advice** will change to **ALLOW** on the Risk Evaluation Results page.

Editing the Default Profile and Performing Risk Evaluation

Using the Sample Application, you can change the DeviceDNA, IP address, and the Device ID of the computer that you are using to simulate various scenarios. To edit the default profile of a user:

1. On the Main Page of the Sample Application, click **Evaluate Risk** to open the Risk Evaluation page.
2. Specify the user name whose profile you want to edit in the **User Name** field.
3. Specify the user's organization in the **User Organization** field.
4. Click **Edit Inputs** to open the Edit Risk-Evaluation Inputs page.
5. On the page, all fields are pre-populated. Change the values for one or more of the required fields:
   - **My User Name**
   - **My Org**
   - **Machine Finger Print of My Device**
   - **IP Address of My Machine**
   - **Device ID of My Machine**
6. Click **Evaluate Risk** to open the Risk Evaluation Results page.
7. Click **Next Step** to open the Post Evaluation page and perform post-evaluation on the specified user profile.
8. Specify the result of secondary authentication by selecting the appropriate option from the **Result of Secondary Authentication** list.
9. Click **Post Evaluate** to complete post evaluation and display the result of the same.

Note: To ensure secure communication between RiskFort components, you can configure them to support SSL (Secure Socket Layer) transport mode. See Appendix F, "Configuring SSL" for more information.

Post-Installation Checklist

Arcot recommends that you fill this checklist (Table 4-2) with the installation and setup information for RiskFort. You will need this information for various administrative tasks that you will perform later.

Table 4-2. Installation Checklist

Your Information	Example Entry	Your Entry
ARCOT_HOME	C:\Program Files\Arcot Systems	
SYSTEM INFORMATION		
Host Name	my-bank	
User Name	administrator	
Password	password1234!	
Configured Components	RiskFort Server Administration Console User Data Service	
ADMINISTRATION CONSOLE INFORMATION		
Host Name	localhost	
Port	8080	
Master Administrator Password	mypassword1234!	
USER DATA SERVICE INFORMATION		
Host Name	localhost	
Port	8080	
Application Context Root	arcotuds	

Chapter 5
Deploying RiskFort on a Distributed System

Use the **Arcot RiskFort 2.2.6 InstallAnywhere Wizard** to install RiskFort components. This Wizard supports *Complete* and *Custom* installation types. However, to install and configure RiskFort in a distributed environment, you must use the **Custom** option when you run the installer.

The following steps provide a quick overview of the process:

1. Run the RiskFort installer to install RiskFort Server and Administration Console and to configure them to access your SQL database. You can also choose to install the Web Services on the same system.

   See "Installing on the First System" for installation instructions.

2. Execute the database scripts to create RiskFort schema and database tables. Also ensure that the database setup was successful.

   See "Creating a Data Source Name (DSN)", "Running Database Scripts" and "Verifying the Database Setup" for more information.

3. Deploy Web applications (UDS and Administration Console) on the application server and verify the deployments.

   See "Deploying Web Applications" for more information.

4. Log in to Administration Console with the Master Administrator credentials to initialize RiskFort.

   See "Logging in to Administration Console" and "Bootstrapping the System" for more information.

5. Start the RiskFort Server and the Case Management Queuing Server, and verify if they start successfully.

   See "Starting RiskFort Server", "Starting the Case Management Queuing Server", and "Verifying the Installation" for more information.

6. (Optional) To ensure secure communication between RiskFort components, you can configure them to support SSL (Secure Socket Layer) transport mode.

   See Appendix F, "Configuring SSL" for more information.

7. Install the Java SDKs and Web Services on one or more systems.

See "Installing on the Second System" for more information.

8. Deploy, configure, and use Sample Application to test RiskFort configuration.

Note: To install the Sample Application *only*, you must ensure that you select only the **SDKs and Sample Application** option and proceed with the installation.

See "Deploying Sample Application", "Configuring Sample Application for Communication with RiskFort Server", and "Using Sample Application" for more information.

9. Complete the installation checklist.

See "Post-Installation Checklist" for more information.

Important Notes Related to Installation

You must keep the following points in mind while installing RiskFort either on a single system or in a distributed environment:

- You must ensure that the `<install_location>` *must not contain* any special characters (such as `~ ! @ # $ % ^ & * ( ) _ + = { }[ ] ' "`).
- RiskFort 2.2.6 does not support upgrade from a previous version (1.7 or earlier). Also, you cannot install RiskFort 2.2.6 over a previously installed version.
- Currently, you cannot modify or repair RiskFort components by using the installer. You *must* uninstall the component and then re-install it.
- Do not close the installer window, if the installation is in progress. If at any time during installation (*especially during the last stages*), if you click the **Cancel** button to abort the installation, then the installer might not remove *all* the directories it has created so far. You will manually need to clean up the installation directory, `<install_location>\Arcot Systems\` and its subdirectories.

Installing on the First System

To install (and later configure) RiskFort on Windows successfully, the user account that you plan to use for installation *must* belong to the `Administrators` group. Else, some critical steps in the installation, such as DSN creation and configuration and RiskFort service creation, will not go through successfully, though the installation might go through without any errors.

In a distributed scenario, depending on how many systems you are distributing RiskFort, Administration Console, Java SDKs, and Web Services, typically you install RiskFort Server on the first system. *Custom installation* allows you to install only the selected components from the package. This option is recommended for advanced users.

Note: Before proceeding with the installation, ensure that all prerequisite software components are installed and the database is set up, as described in the Chapter 3, "Preparing for Installation".

Perform the following tasks to install RiskFort components:

1. Navigate to the directory where the `Arcot-RiskFort-2.2.6-Windows-Installer.exe` file is located and double-click the file to run the installation wizard.

   The Welcome screen appears.

2. Click **Next** to continue.

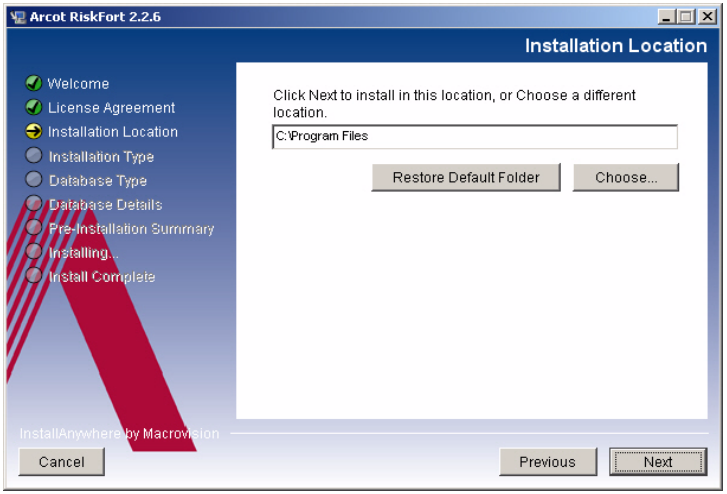
   The License Agreement screen appears.

3. Read the license agreement carefully, select the **I accept the terms of the License Agreement** option, and click **Next.**

   The installer now checks if any other Arcot product is installed on the computer.

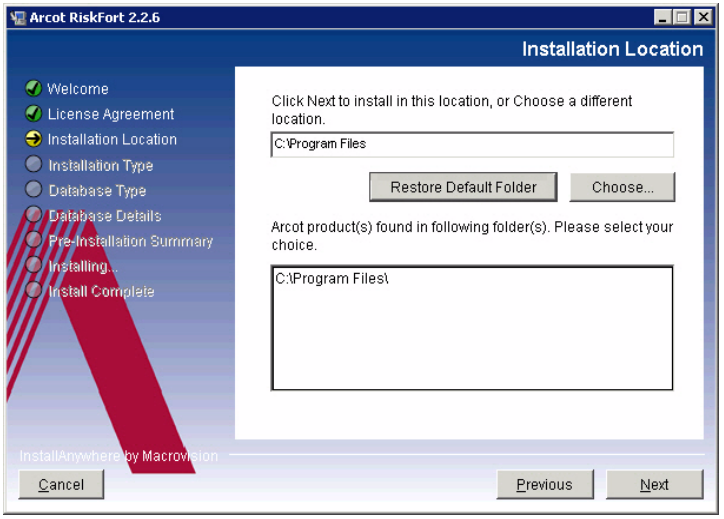
   If it does not find an existing Arcot product installation, then you will be prompted for an installation directory. In this case, the Installation Location screen, shown in the Figure 5-1, appears.

Figure 5-1 Installation Location Screen: No Installation Detected



If the installer detects an existing Arcot product installation, then you will not be prompted for an installation directory. Figure 5-2 appears when an existing `ARCOT_HOME` was located on the computer.

Figure 5-2 Installation Location Screen: Previous Installation Detected



4. You can accept the default directory specified by the installer to install RiskFort. You can also click **Choose** to navigate and to specify a different directory.

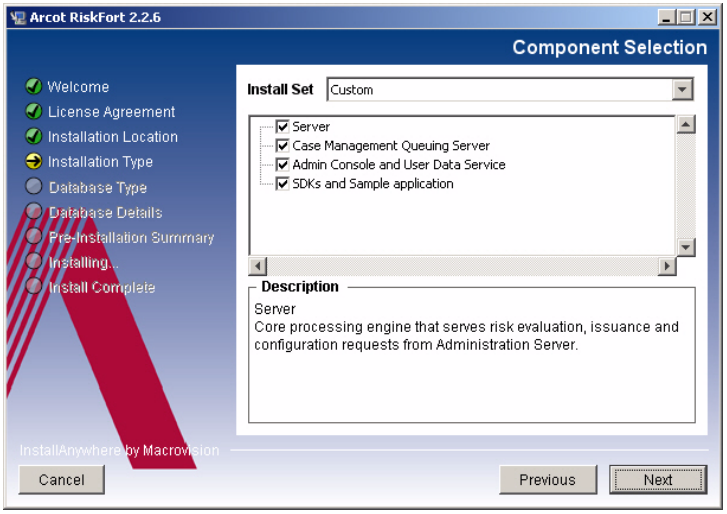
   Click **Next** to install in the specified directory.

   The Installation Type screen appears.

5. Click **Custom** to install the selected components in one `ARCOT_HOME`.

   The Component Selection screen appears, as shown in the Figure 5-3.

   Figure 5-3 Component Selection Screen



6. Deselect the components that are not required. By default, all components are selected for installation.

   For example, to install RiskFort Server, Case Management Queuing Server, and the Administration Console (*without* the SDKs and the Sample Application) on the current system, you will need to:

   a. Select the **RiskFort Server** option.

   b. Select the **Case Management Queuing Server** option.

   c. Select the **Administration Console and User Data Service** option.

d. Deselect the **SDKs and Sample Application** option.

Note: To install the Sample Application *only*, you must select the **SDKs and Sample Application** option and proceed with the installation.

Table 5-1 describes all components that are installed by the RiskFort installer.

Table 5-1. Components Installed by RiskFort

Component	Description
Server	This option installs the core Processing engine (**RiskFort Server**) that serves the following requests from Administration Console: • Risk Evaluation • Issuance • Configuration In addition, this component also installs the following Web services that have been built into the server: • **Risk Evaluation Web Service** - Provides the Web-based programming interface for risk evaluation with RiskFort Server. • **Issuance Web Service** - Provides the Web-based programming interface for creation and management of users. • **Administration Web Service** - Provides the Web-based programming interface used by the RiskFort Administration Console.
Case Management Queuing Server	This option installs the core Queuing engine (**Case Management Queuing Server**) that allocates cases to the Customer Support Representatives (CSRs) who work on these cases. **Note:** At any given point in time, *all* instances of Administration Console can only connect to this single instance of the Case Management Queuing Server.

Table 5-1. Components Installed by RiskFort

Component	Description
Administration Console and User Data Service	This option provides Web-based interface for Server configurations and for administration of rules and users. This package comprises the following sub-components: • **Administration Console** - Provides the Web-based interface for managing RiskFort Server and risk evaluation-related configurations. • **User Data Service (UDS)** - Acts as an abstraction layer for accessing different types of user repositories, such as relational databases (RDBMSs) and directory servers (LDAPs.)
SDKs and Sample Application	This option provides programming interfaces (in form of APIs and Web Services) that can be invoked by your application to forward risk evaluation and user issuance requests to the RiskFort Server. This package comprises the following sub-components: • **RiskFort SDK** - Provides the Java programming interface for risk evaluation with RiskFort Server. • **Issuance SDK** - Provides the Java programming interface for creation and management of users. • **Sample Application** - Demonstrates the usage of RiskFort Java APIs. In addition, it can also be used to verify if RiskFort was installed successfully, and if it is able to perform risk evaluation and issuance requests. Refer to Chapter 6, "Configuring RiskFort SDKs and Web Services" for more information on configuring these components.

Note: If RiskFort Evaluation was not selected for installation on this screen, then screens in Step 7 through Step 9 will not appear.

7. Select **Next** to continue.

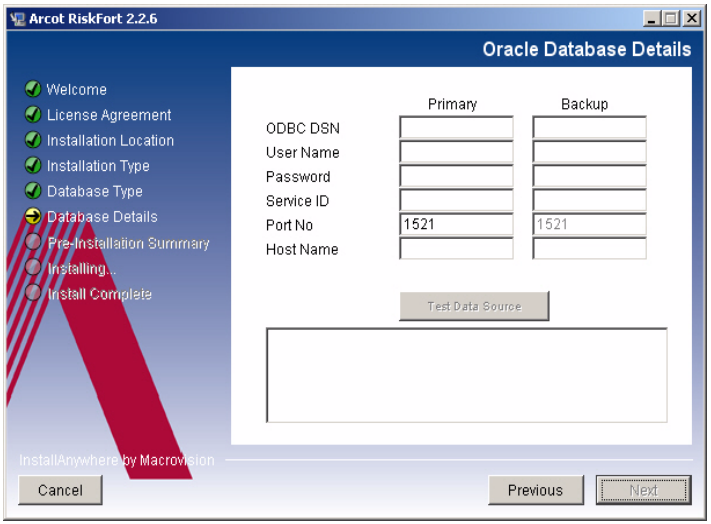
   The Database Type screen appears.

8. Depending on the type database you have, you can either select **Oracle** or **Microsoft SQL**. Click **Next** to proceed.

   If you selected **Oracle** on the Database Type screen, then the Oracle Database Details (Figure 5-4) screen appears.

Database Source Name (DSN) specifies the information required to connect to a database by using an ODBC driver. This information includes database name, directory, database driver, User ID, and password.

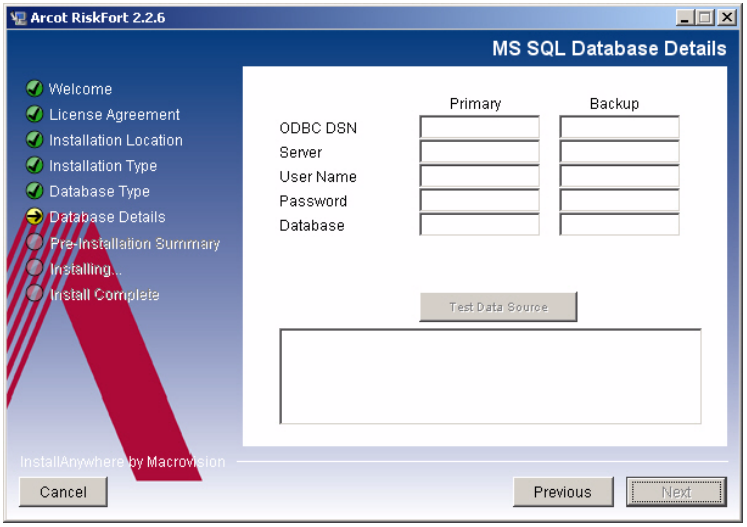
Figure 5-4 Oracle Database Details Screen



If you selected **Microsoft SQL** on the Database Type screen, then the MS SQL Database Details screen (Figure 5-5) appears. This screen slightly differs from the Oracle Database Details screen.

	Note: If you are using MS SQL database, then you must ensure that the ODBC Driver version you are using is same as mentioned in the "Configuring Database Server" in Chapter 3 section.

Figure 5-5 MS SQL Database Details Screen



9. **For Oracle** Primary and Backup databases, fill in the following information in the fields (Figure 5-4):

   - **ODBC DSN:** The name of the DSN, which refers to the RiskFort datastore. This value is used by the RiskFort Server to connect to the RiskFort datastore. The recommended value to enter is `arcotdsn`.
   - **User Name:** The database user name for RiskFort to access the database. This name is specified by the database administrator.

     This user *must* have the `create session` and DBA rights.

Important: The **User Name** value for the Primary and Backup DSNs *must* be different.

   - **Password:** The password associated with the **User Name** you specified in the previous field and which is used by RiskFort to access the database. This password is specified by the database administrator.
   - **Service ID:** The Oracle System Identifier (SID) that refers to the instance of the Oracle database running on the server.

- **Port:** The port at which the specified database listens to incoming requests. The default port at which an Oracle database listens is `1521`. However, if you would like to specify another port, enter the port value in this field.
- **Host Name:** The host name or IP address of the RiskFort datastore.

  Syntax: `<server_name>`

  Example: `demodatabase`

For MS SQL Primary and Backup databases, fill in the following information in the fields (Figure 5-5)

- **ODBC DSN:** The name of the DSN, which refers to the RiskFort datastore. This value is used by the RiskFort Server to connect to the RiskFort datastore. The recommended value to enter is `arcotdsn`.
- **Server:** The host name or IP address of the RiskFort datastore.
  - **Default Instance**

    Syntax: `<server_name>`

    Example: `demodatabase`
  - **Named Instance**

    Syntax: `<server_name>\<instance_name>`

    Example: `demodatabase\instance1`
- **User Name:** The database user name for RiskFort Server to access the datastore. This name is specified by the database administrator. (MS SQL Server, typically, refers to this as `login`.)

  This user *must* have the `create session` and DBA rights.

Important: The **User Name** value for the Primary and Backup DSNs *must* be different.

- **Password:** The password associated with the **User Name** you specified in the previous field and which is used by RiskFort to access the datastore. This password is specified by the database administrator.
- **Database:** The name of the MS SQL database instance.

10. To test if the connection to the specified database was successful, click the **Test Data Source** button. After completing the test, click **Next** to continue.

The Pre-Installation Summary screen appears.

Review the information on this screen, and if you need to change a previous selection, then click **Previous** to do so. After changing the required selection, click **Next** to go to the next screen.

11. Click **Install** to begin the installation.

    The Installing Arcot RiskFort screen appears. This might take several minutes. After some time the Installation Complete screen appears.

12. Click **Yes** to restart the computer.

    RiskFort Server launches correctly only *after* the computer has been restarted.

13. Click **Done** to complete the installation.

Note: After the installation is completed, perform the post-installation tasks discussed in following sections.

Installation Logs

After installation, you can access the installation log file (`Arcot_RiskFort_InstallLog.log`) at the following directory:

`<install_location>\Arcot Systems\logs\`

If for some reason, the installation failed, then the error log is available in the same location where you ran the Installer from.

Performing Post-Installation Tasks on the First System

This section guides you through the post-installation tasks that you must perform after installing RiskFort on the first system. These steps are required for configuring RiskFort correctly and must be *performed in the following order*:

1. Creating a Data Source Name (DSN)
2. Running Database Scripts
3. Verifying the Database Setup
4. Deploying Web Applications
5. Logging in to Administration Console

6. Bootstrapping the System
7. Starting RiskFort Server
8. Starting the Case Management Queuing Server
9. Verifying the Installation

Note: After completing these post-installation tasks, perform the SDK and Web Services configuration tasks discussed in Chapter 6, "Configuring RiskFort SDKs and Web Services".

Creating a Data Source Name (DSN)

To create the DSN for your Microsoft SQL Server or the Oracle Database Server:

1. Open the Control Panel, navigate to **Administrative Tools, Data Sources (ODBC), System DSN**, and click **Add**.
2. Select the required DSN type, and click **Finish**.
3. Create the DSN for the database by using the details provided in Step 9 on page 5-81.
4. Click **OK** to create the DSN.

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

Running Database Scripts

Important: Before you run the scripts discussed in this section, you must ensure that you are logged in as the same database user that you created in the "Configuring Database Server" in Chapter 3 section.

RiskFort is shipped with scripts that are required to create necessary tables in the RiskFort database. To run the required database scripts:

1. Navigate to the following directory:

   `<install_location>\Arcot Systems\dbscripts\`

2. Based on the database you are using, navigate to one of the following directories:
   - **For Oracle:**

     `<install_location>\Arcot Systems\dbscripts\oracle\`

- **For MS SQL:**

  `<install_location>\Arcot Systems\dbscripts\mssql\`

3. Run the scripts *in the following order*:
   - `arcot-db-config-for common-1.0.sql`
   - `arcot-db-config-for-riskfort-2.2.6.sql`

Verifying the Database Setup

After running the required database scripts, you must verify whether the RiskFort schemas were seeded correctly. To do so:

1. Log in to the RiskFort database as a user with `SYSDBA` privileges.
2. Run the following query:

   ```
   SELECT SERVERNAME, VERSION FROM ARRFSERVERS;
   ```

   You must see the following output as a result of the preceding query:

   ```
   SERVERNAME                    VERSION
   ------------------------  ----------------
   RiskFort                       2.2.6
   RiskFortCaseManagement         2.2.6
   ```

3. Log out of the database console.

Deploying Web Applications

Two components of RiskFort, User Data Service (UDS) and Administration Console, are Web-based and can be deployed on any of the following supported application servers:

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Before you deploy the WAR files for these Web applications on the application server of your choice, you must copy the Arcot-proprietary files required by UDS and Administration Console to the appropriate location on your application server. This section walks you through the steps to copy the required crypto-files to your application server and to deploy the WAR files of these Web applications:

1. Preparing Your Application Server

2. (Optional) Creating Enterprise Archive Files
3. Deploying User Data Service (UDS)
4. Verifying UDS Deployment
5. Deploying Administration Console
6. Verifying Administration Console Deployment

Preparing Your Application Server

UDS and Administration Console use the following files to access the RiskFort database securely:

- `arcot-crypto-util.jar` available at:

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

- `ArcotAccessKeyProvider.dll` available at:

  `<install_location>\Arcot Systems\java\ext\win\<32\or\64\bit>\`

As a result, these files must be copied to the appropriate location on the application server where you have deployed these RiskFort components. The following subsections provide information on copying these files for:

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Apache Tomcat

To copy the Arcot-proprietary files:

1. Copy `arcot-crypto-util.jar` *to* `%JAVA_HOME%\jre\lib\ext\`.
2. Copy `ArcotAccessKeyProvider.dll` *to:* `%JAVA_HOME%\jre\bin\`.
3. Restart the application server.

IBM WebSphere

To copy the Arcot-proprietary files:

1. Log into WebSphere Administration Console.
2. Click **Environment,** and then click **Shared Libraries**.
   a. From the **Scope** drop-down, select a valid visibility scope. The scope must include the target server or node on which the application is deployed.

b. Click **New**.

c. Enter the **Name**, for example, *ArcotJNI*.

d. Specify the **Classpath**.

This path must point to the location where the `arcot-crypto-util.jar` file is present and must also include the file name. For example, `C:\Program Files\Arcot Systems\ext\`**`arcot-crypto-util.jar`**.

e. Enter the JNI Library path.

This path must point to the location where the `ArcotAccessKeyProvider.dll` file is present.

3. Click **Apply** to save the changes.
4. Configure the server-level class loaders.
   a. Click **Servers**, and then click **Application Servers.**
   b. Under **Application Servers** access the settings page of the server for which the configuration are performed.
   c. Click **Java and Process Management** and then click **Class Loader**.
   d. Click **New**.
   e. Select default **Classes loaded with parent class loader first** and click **OK.**
   f. Click the auto-generated **Class Loader ID**.
   g. On the class loader **Configuration** page, click **Shared Library References**.
   h. Click **Add**, select **ArcotJNI,** and then click **Apply**.
   i. Save the changes made.
5. Copy `ArcotAccessKeyProvider.dll` to `<`*`WebSphere_JAVA_HOME`*`>\jre\`**`bin`**`\`.
6. Restart WebSphere.

BEA WebLogic

To copy the Arcot-proprietary files:

1. Copy `ArcotAccessKeyProvider.dll` to WebLogic's `<`*`WebLogic_JAVA_HOME`*`>\jre\`**`bin`**`\`.

2. Copy `arcot-crypto-util.jar` to WebLogic's `<WebLogic_JAVA_HOME>\jre\lib\ext\`.

Note: Ensure that you use the appropriate `<JAVA_HOME>` used by WebLogic.

3. Login to WebLogic Administration Console.
4. Navigate to **Deployments**.
5. Enable the **Lock and Edit** option.
6. Click **Install** and navigate to the directory that contains the `arcot-crypto-util.jar` file.
7. Click **Next** to open the Application Installation Assistant.
8. Click **Next** to display the Summary page.
9. Click **Finish**.
10. Activate the changes.
11. Restart the server.

(Optional) Creating Enterprise Archive Files

By default, Arcot provides Web ARchive (WAR) files to deploy UDS and Administration Console. However if required, you can also change the format of these files to Enterprise ARchive (EAR) and then deploy the EAR files.

As discussed in the following subsections, you can either generate separate EAR files for both UDS and Administration Console, or you can generate a single EAR file that contains both Web archives.

Generating Separate EAR Files

To create separate EAR files for UDS and Administration Console:

1. Open the Command Prompt window.
2. Navigate to the `<install_location>\Arcot Systems\tools\bundlemanager\` directory.
3. Run the following command to create the EAR file:

```
java -jar bundle-manager.jar -ear <filename.ear> -warList
<filename.war>
```

The preceding command generates individual EAR files that are available at:

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

Generating a Single EAR File

To create a single EAR file that contains the UDS and Administration Console Web archives:

1. Open the Command Prompt window.
2. Navigate to the `<install_location>\Arcot Systems\tools\bundlemanager\` directory.
3. Run the following command to create the EAR file:

   ```
   java -jar bundle-manager.jar -ear <filename.ear> -warList
   arcotadmin.war arcotuds.war
   ```

   The preceding command generates a single EAR file that is available at:

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

Deploying User Data Service (UDS)

User Data Service (UDS) enables access to the third-party data repositories (LDAP directory servers) deployed by your organization. As a result, it enables RiskFort Server and the Administration Console to seamlessly access your existing data. If the LDAP directory server is not configured, then it accesses the RiskFort database to read the user information. (See Step 3 on page 5-95 in the bootstrapping steps to know about the parameters that must be set to connect UDS to other RiskFort components.)

You need the `arcotuds.war` file to deploy User Data Service (UDS). To deploy UDS by using this file:

1. Deploy `arcotuds.war` on the application server. This file is available at:

   Note: The deployment procedure depends on the application server that you are using. Refer to your application server vendor documentation for detailed instructions.
   For example, in case of Apache Tomcat, you must deploy the WAR file at `<APP_SERVER_HOME>\webapps\`.

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

2. (**For WebSphere Only**) Configure to reload the UDS class when the application files are updated.

a. Navigate to **Application**, **Enterprise Applications** and access the UDS settings page.

b. Under **Class loader order**, select the **Classes loaded with local class loader first (parent last)** option.

c. Under **WAR class loader policy**, select the **Single class loader for application**.

d. Click **Apply** to save the changes.

3. Restart the application server.

Verifying UDS Deployment

The `arcotuds.log` file is used for logging UDS-related information. To verify if UDS started correctly:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotuds.log` file in any editor and locate the following lines:

   - `Initializing Arcot User Data Service (Version: 1.0.9)`
   - `Arcot User Data Service initialized successfully.`

   These lines indicate that UDS was deployed successfully.

Note: You might also want to make sure that the log files *do not* contain any `FATAL` *and* `WARNING` messages.

Deploying Administration Console

The *Administration Console* is a browser-based interface to RiskFort that enables you to customize the server configurations and manage the deployed system.

Note: To manage RiskFort by using Administration Console, you must ensure that Administration Console can access the system where the RiskFort Server is installed by its `hostname`.

You need the `arcotadmin.war` file to deploy the RiskFort Administration Console. This file is available at:

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

To deploy the Administration Console WAR file on your application server:

1. Deploy `arcotadmin.war` in the appropriate directory on the application server.

Note: The deployment procedure depends on the application server that you are using. Refer to your application server vendor documentation for detailed instructions.
For example, in case of Apache Tomcat, you must deploy the WAR file at `<APP_SERVER_HOME>\webapps\`.

2. Restart the application server.

Verifying Administration Console Deployment

The `arcotadmin.log` file is used for logging the Administration Console information.

To verify if the Administration Console was deployed successfully:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotadmin.log` file in any editor and locate the following lines:

   - `Arcot Administration Console v1.0.9`
   - `Arcot Administration Console Configured Successfully.`

   These lines indicate that your Administration Console was deployed successfully.

Note: You might also want to make sure that the log files *do not* contain any `FATAL` *and* `WARNING` messages.

Logging in to Administration Console

When logging in to the Administration Console for the first time, you *must* use the **Master Administrator** (MA) credentials that are configured automatically in the database during the deployment.

To log in to the Administration Console as MA:

1. Start the Administration Console in a Web browser window. The default URL for the Administration Console is:

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

Note: The host and port information that you specify in the preceding URL must be of the application server where you deployed the Administration Console.

2. Log in by using the default Master Administrator account credentials. The credentials are:
   - **User Name: masteradmin**
   - **Password: master1234!**

Important: Arcot strongly recommends that you change the Master Administrator password after the first log in.
Refer to the *Arcot RiskFort Administration Guide* for more information on changing the administrator password.

Bootstrapping the System

Before you can start using the Administration Console to manage RiskFort, you must first perform the following mandatory steps to initialize the system:

- Change the default Master Administrator password
- Set up UDS connectivity parameters
- Specify the authentication mechanism for the Default organization

Bootstrapping is a Wizard-driven process that walks you through these setup tasks. Other administrative links are enabled only after you perform these tasks.

Before you proceed with "Performing Bootstrapping Tasks", you must understand the related concept of "Default Organization".

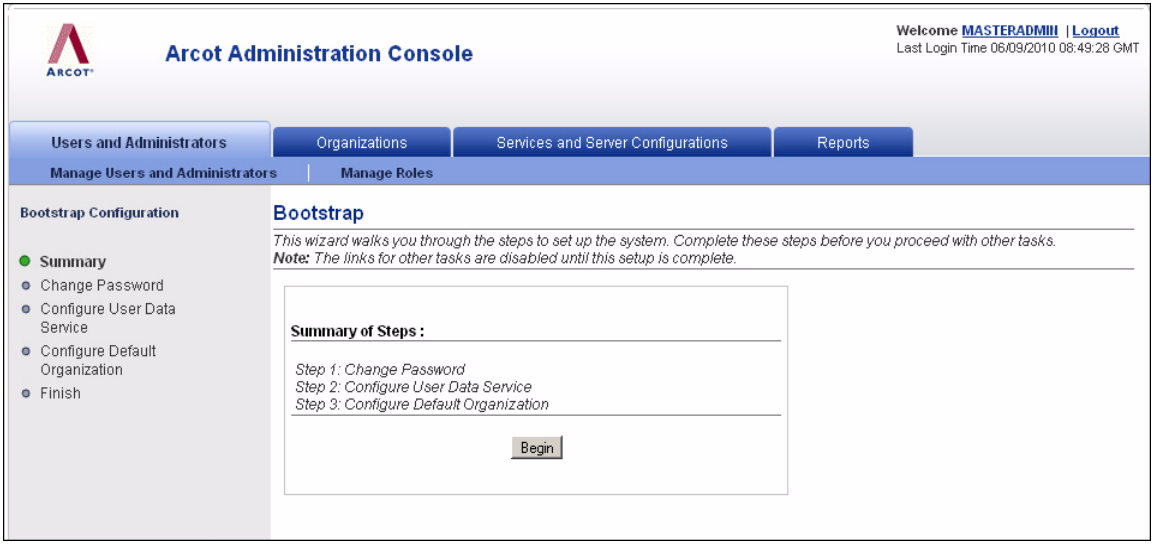
Default Organization

When you deploy the Administration Console, an organization is created automatically. This organization is referred to as *Default Organization* (`DEFAULTORG`). As a single-organization system, the Default Organization itself can be used without creating any new organizations.

Performing Bootstrapping Tasks

When you first log in to the Administration Console as the Master Administrator (MA), the Summary screen for the Bootstrap wizard screen (Figure 5-6) appears.

Figure 5-6 Bootstrap Wizard: Summary Screen

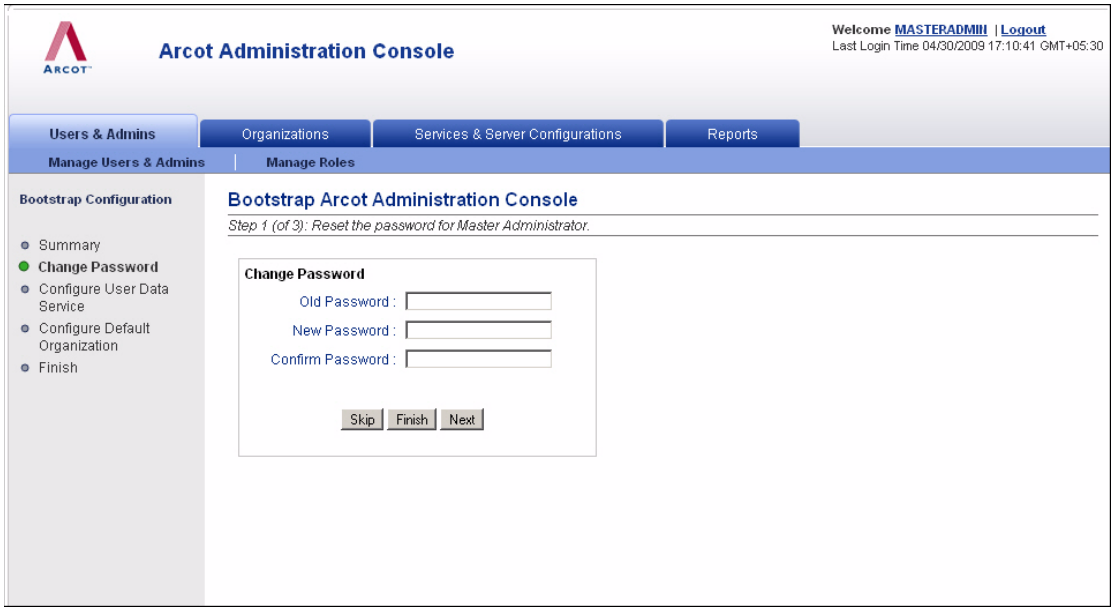


To bootstrap the system using the wizard:

1. Click **Begin** to start the process.

   The Change Password screen, as shown in Figure 5-7, appears.

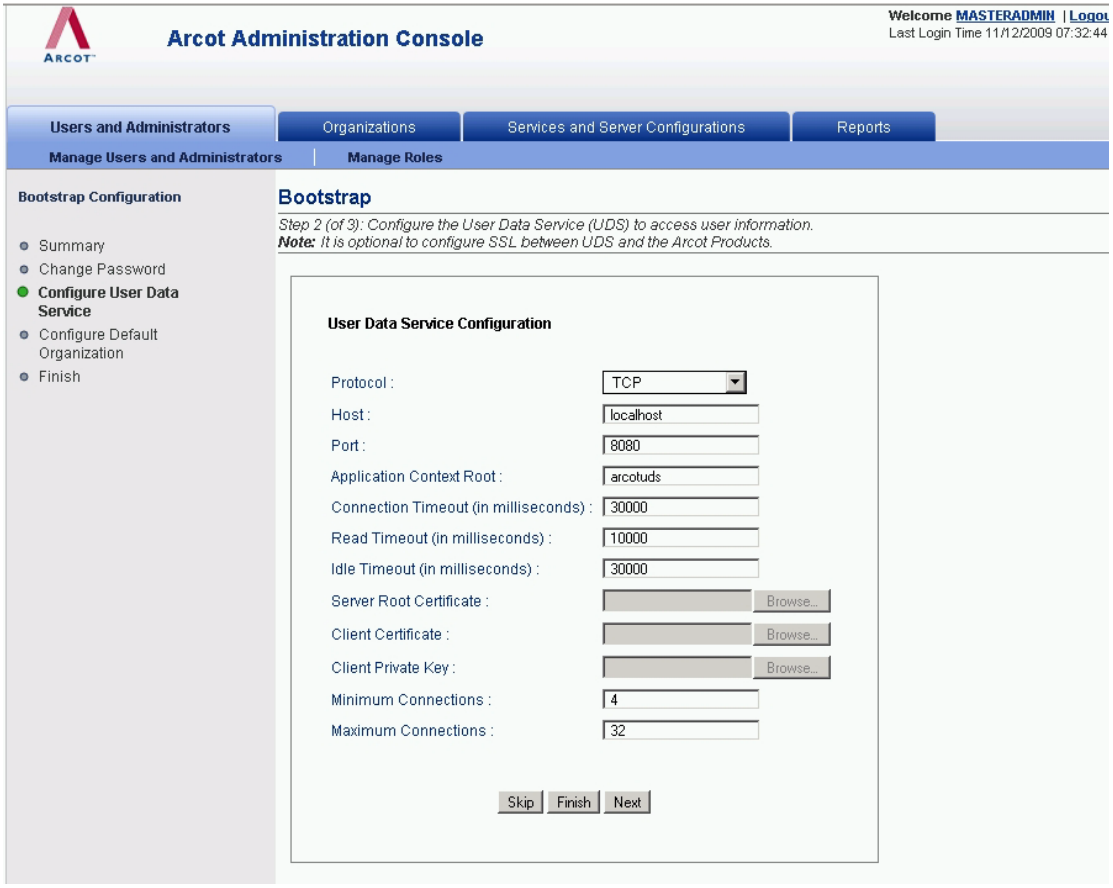
Figure 5-7 Bootstrap Wizard: Change Password Screen



2. Specify the **Old Password**, **New Password**, **Confirm Password**, and click **Next.**

   The Configure User Data Service screen, as shown in Figure 5-8, appears.

Figure 5-8 Bootstrap Wizard: Configure User Data Service Screen



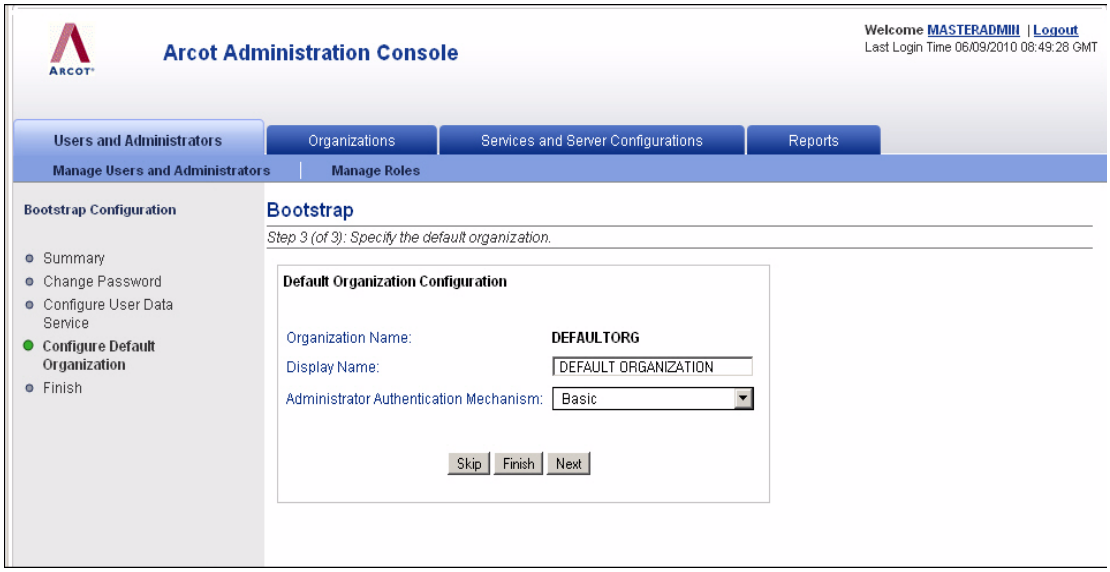
3. Specify the parameters listed in Table 5-2 to configure UDS:

Table 5-2. UDS Configuration Parameters

Parameter	Default Value	Description
Protocol	TCP	The protocol to connect to the UDS using the Administration Console. The available options are: • `TCP` • `One way SSL` • `Two way SSL`
Host	localhost	The host name or the IP address of the application server where the UDS is deployed.
Port	8080	The port on which the application server is available.
Application Context Root	arcotuds	The tag that is used to define UDS in the application server. For example, the context root in the *http://<host>:<port>/arcotuds/services* URL is `arcotuds`.
Connection Timeout (in milliseconds)	30000	Maximum time in **milliseconds** before the UDS service is considered unreachable.
Read Timeout (in milliseconds)	10000	Maximum time in **milliseconds** to wait for a response from UDS.
Idle Timeout (in milliseconds)	30000	Maximum time in **milliseconds** after which an idle connection will be closed.
Server Root Certificate	No Default	Upload the CA certificate file of UDS server. The file must be in PEM format.
Client Root Certificate	No Default	Upload the CA certificate file of the RiskFort Server. The file must be in PEM format.
Client Private Key	No Default	The location of file that contains the CA's private key.
Minimum Connections	4	The minimum number of connections that will be created between the RiskFort Server and UDS.
Maximum Connections	32	The maximum number of connections that can be created between the RiskFort Server and UDS.

The Configure Default Organization screen, shown in Figure 5-9, appears.

Figure 5-9 Bootstrap Wizard: Configure Default Organization Screen



4. Specify the following parameters for the Default Organization:
   - **Display Name:** The descriptive name of the organization. This name appears on all other Administration Console pages and reports.
   - **Authentication Mechanism:** The mechanism that is used to authenticate administrators belonging to the Default Organization. Administration Console supports two types of authentication methods for the administrators to log in:
     - **Basic User Password**

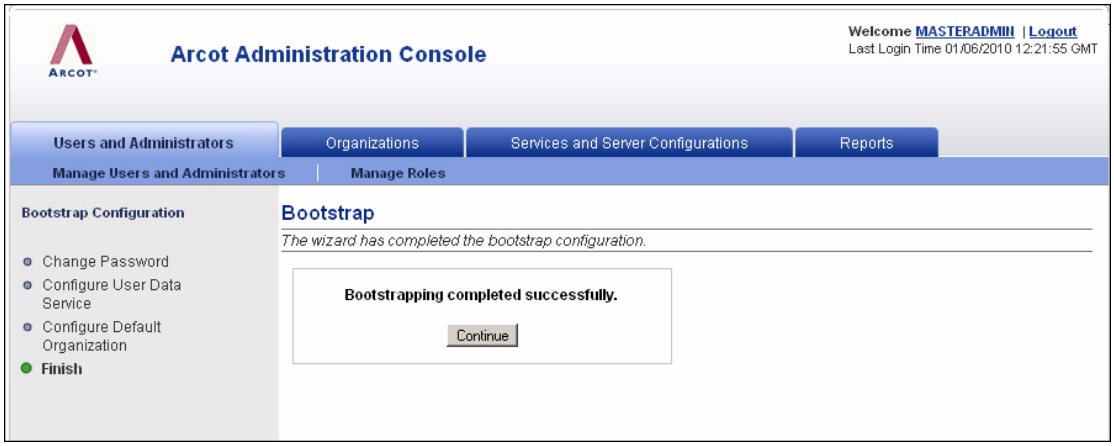
       If you choose this option, then the built-in authentication method provided by the Administration Console is used for authenticating the administrators.
     - **WebFort User Password**

       If you select the **WebFort User Password** option here, then the credentials are issued and authenticated by the WebFort Server. For this, the Arcot WebFort Server must be installed.

	Book: See the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on installing and configuring WebFort.

The Administration Console initialization is completed, as indicated in the Finish screen (Figure 5-10).

Figure 5-10 Bootstrap Wizard: Finish Screen



5. Click **Continue** to proceed with other configurations using the Administration Console.

Starting RiskFort Server

To start the RiskFort Server:

1. Click the **Start** button on your desktop window.
2. Navigate to **Settings, Control Panel, Administrative Tools,** and then **Services.**
3. Locate and double-click **Arcot RiskFort Service**.
4. Click **Start** in the service's window.

Note: If you want to stop the RiskFort Server, then follow the Steps 1 through 3, and click the **Stop** button in the service's window.

Starting the Case Management Queuing Server

To **start** the Case Management Queuing Server:

1. Click the **Start** button on your desktop window.
2. Navigate to **Settings, Control Panel, Administrative Tools,** and then **Services.**

3. Locate and double-click the **Arcot RiskFort Case Management Queuing Service**.
4. Click **Start** in the service's window.

Note: If you want to stop the Case Management Queuing Server, then follow the Steps 1 through 3, and click the **Stop** button in the service's window.

To **verify** if the Case Management service started successfully:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotriskfortcasemgmtserver.log` file in any editor and locate the following lines:

   - `STARTING Arcot RiskFort Case Management 2.2.6_w`
   - `Arcot RiskFort Case Management Service READY`

Note: You might also want to make sure that the log file does not contain any `FATAL` and `WARNING` messages.

Verifying the Installation

To verify if the server started correctly:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs\`

2. Open the `arcotriskfort.log` file in any editor and locate the following lines:

   - `STARTING Arcot RiskFort 2.2.6_w`
   - `Arcot RiskFort Service READY`

Note: You might also want to make sure that the log file does not contain any `FATAL` and `WARNING` messages.

Installing on the Second System

After installing RiskFort Server and Administration Console, you must now install the other remaining components on the second system in this distributed environment. The specific components to install must have been determined when you performed your planning in Chapter 2, "Planning the Deployment".

Before proceeding with the installation, ensure that all prerequisite software components are installed on this system as described in Chapter 3, "Preparing for Installation".

To install RiskFort components on the subsequent system:

1. Copy the installer file `Arcot-RiskFort-2.2.6-Windows-Installer.exe` on the target (second) system.
2. Double-click the installer to run it.
3. Follow the installer instructions from Step 2 on page 5-75 until you reach the **Choose Install Set** screen (Figure 5-3 on page 5-77).
4. Select the components you wish to install.

   Typically, you will be installing the Java SDKs for Risk Evaluation and Issuance.
5. After you have selected all the components, follow the from Step 7 on page 5-79 through Step 13 to complete the installation.

Performing Post-Installation Tasks on the Second System

Perform the following post-installation on the second system, where you have installed Java SDKs and Web Services:

1. Deploying Sample Application
2. Configuring Sample Application for Communication with RiskFort Server
3. Using Sample Application

Note: After you complete these configurations, you must then configure RiskFort SDKs (and Web services), as discussed in Chapter 6, "Configuring RiskFort SDKs and Web Services".

Deploying Sample Application

Sample Application can be used to verify if RiskFort was installed and configured properly. In addition, it demonstrates:

- The typical RiskFort workflows
- Basic operations (invocation and post-processing) of RiskFort APIs
- Integration of your application with RiskFort

Important: Sample Application *must* be deployed on the same application server where Risk Evaluation and Issuance SDKs are Installed.

Note: If you did not install Sample Application during installation, then you can install *only* the Sample Application by running the installer again and by selecting the **SDKs and Sample Application** options and proceed with the installation.

To deploy the Sample Application:

1. Navigate to **Settings, Control Panel, Administrative Tools,** and the select **Services.**
2. Stop the application server services.
3. Deploy the `riskfort-2.2.6-sample-application.war` file from `the following location:`

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

   Note: Although you will also see `riskfort-2.2.6-sample-application.war` in the package, it is recommended that you deploy the Sample Application file from the preceding location.

4. Navigate to **Settings, Control Panel, Administrative Tools,** and then select **Services.**
5. Restart the application server.

Configuring Sample Application for Communication with RiskFort Server

The `riskfort.risk-evaluation.properties` file provides the parameters for the Java SDK and Sample Application to read RiskFort Server information. Therefore, after deploying the Sample Application, you must now configure it to communicate with RiskFort Server. This file is only available *after* you deploy the RiskFort Sample Application WAR file, `riskfort-2.2.6-sample-application.war`.

To configure the `riskfort.risk-evaluation.properties` file:

1. Navigate to the `riskfort.risk-evaluation.properties` file on your application server.

   In case of Apache Tomcat this file is available at:

   `<App_Home/`**`riskfort-2.2.6-sample-application`**`>/WEB-INF/classes/`**`properties`**`/`

   Here, `<App_Home/`**`riskfort-2.2.6-sample-application`**`/>` represents the directory path where RiskFort application WAR files are deployed.

2. Open the `riskfort.risk-evaluation.properties` file in an editor window and set the value for following parameters:

   - `HOST.1`
   - `PORT.1`

     A default value is specified for the remaining parameters in the file. You can change these values, if required. See "riskfort.risk-evaluation.properties" in Appendix B for more information on configuration parameters.

3. (**Optional:** Perform this step only if you configured SSL-based communication in Appendix F, "Configuring SSL")

   Set the following parameters:

   - `TRANSPORT_TYPE=SSL` (By default, this parameter is set to `TCP`.)
   - `CA_CERT_FILE=<absolute_path_of_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`

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.

4. Save the changes and close the file.
5. Restart the application server to reflect these changes.

Using Sample Application

This sub-section describes the risk-evaluation operations that can be performed using Sample Application. Each operation in the sample application is designed to run without error when RiskFort is completely installed and functional.

Sample Application demonstrates the following operations that RiskFort Issuance and RiskFort Server can perform:

- Performing Risk Evaluation and Post Evaluation for a First-Time User
- Creating Users
- Performing Risk Evaluation and Post Evaluation for a Known User
- Editing the Default Profile and Performing Risk Evaluation

Performing Risk Evaluation and Post Evaluation for a First-Time User

To perform risk evaluation on the default profile of a user:

1. Ensure that Sample Application is open (in a Web browser window.) The default URL for Sample Application is:

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp
2. Click **Evaluate Risk** to open the Risk Evaluation page.
3. On the page, specify the name of the user (who you want to evaluate) in the **User Name** field.
4. Specify the name of the organization to which the user belongs in the **User Organization** field.
5. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score, the associated Risk Advice, and lists the rules that are configured for the specified organization. For a first-time user, the result is **ALERT**.

6. Click **Next Step** to open the Post Evaluation page and perform post-evaluation on the specified user profile.

   By using Post evaluation, your application provides feedback to RiskFort Server about the current user and/or the device they are using. RiskFort updates user and/or device attributes and the user-device association based on this feedback, and accordingly assesses risk associated with the transactions for the user in future.

7. Specify the result of secondary authentication by selecting the appropriate option from the **Result of Secondary Authentication** list.
8. Specify the name for the user name-device association in the **Association Name** field.
9. Click **Post Evaluate** to complete the post evaluation process and to display the result of the same in the Post Evaluation Results section.

Creating Users

To create a user:

1. Start the Sample Application in a Web browser window. The default URL for Sample Application is:

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp

   The RiskFort Sample Application page appears.

2. Click **Create User** to open the Create User page.
3. Enter a unique user name and their organization name in the **User Name** and **Organization Name** fields, respectively and click **Create User.** If you do not specify the **Organization Name**, then the user is created in `defaultorg`.

   The "The User is created successfully" message appears if the specified user was successfully added to the database.

4. Click **Main Page** to return to the RiskFort Sample Application page.

Performing Risk Evaluation and Post Evaluation for a Known User

1. On the Main Page of the Sample Application, click **Evaluate Risk** to open the Risk Evaluation page.
2. Specify the name of the user you created in the **User Name** field.
3. Specify the user's organization in the **User Organization** field.
4. Click **Evaluate Risk** to open the Risk Evaluation Results page.

The Risk Advice typically is **INCREASEAUTH**.

5. Click **Next Step** to perform Post Evaluation:
   - Specify the **Result of Secondary Authentication** from the list.
   - Edit the **Association Name**, if required.
6. Click **Post Evaluate** to display the final advice.

   If you repeat Step 1 through Step 4, the **Risk Advice** will change to **ALLOW** on the Risk Evaluation Results page.

Editing the Default Profile and Performing Risk Evaluation

Using the Sample Application, you can change the DeviceDNA, IP address, and the Device ID of the computer that you are using to simulate various scenarios. To edit the default profile of a user:

1. On the Main Page of the Sample Application, click **Evaluate Risk** to open the Risk Evaluation page.
2. Specify the user name whose profile you want to edit in the **User Name** field.
3. Specify the user's organization in the **User Organization** field.
4. Click **Edit Inputs** to open the Edit Risk-Evaluation Inputs page.
5. On the page, all fields are pre-populated. Change the values for one or more of the required fields:
   - **My User Name**
   - **My Org**
   - **Machine Finger Print of My Device**
   - **IP Address of My Machine**
   - **Device ID of My Machine**
6. Click **Evaluate Risk** to open the Risk Evaluation Results page.
7. Click **Next Step** to open the Post Evaluation page and perform post-evaluation on the specified user profile.
8. Specify the result of secondary authentication by selecting the appropriate option from the **Result of Secondary Authentication** list.

9. Click **Post Evaluate** to complete post evaluation and display the result of the same.

Note: To ensure secure communication between RiskFort components, you can configure them to support SSL (Secure Socket Layer) transport mode. See Appendix F, "Configuring SSL" for more information.

Post-Installation Checklist

Arcot recommends that you fill this checklist with the installation and setup information for RiskFort. You will need this information for various administrative tasks that you will perform later.

Table 5-3. Installation Checklist

Your Information	Example Entry	Your Entry
ARCOT_HOME	C:\Program Files\Arcot Systems	
SYSTEM INFORMATION		
Host Name	my-bank	
User Name	administrator	
Password	password1234!	
Configured Components	RiskFort Server Administration Console User Data Service	
ADMINISTRATION CONSOLE INFORMATION		
Host Name	localhost	
Port	8080	
Master Administrator Password	mypassword1234!	
USER DATA SERVICE INFORMATION		
Host Name	localhost	
Port	8080	
Application Context Root	arcotuds	

Chapter 6
Configuring RiskFort SDKs and Web Services

This chapter describes the steps to configure the Application Programming Interfaces (APIs) and Web services provided by RiskFort.

The chapter covers the following topics:

RiskFort APIs

RiskFort is shipped with a set of Java APIs in the form of the Java SDK, which is available in the following location:

`<install_location>\Arcot Systems\sdk\java\lib\arcot\`

The APIs shipped with RiskFort include:

Risk Evaluation API

RiskFort SDK (`arcot-riskfort-evaluaterisk.jar`) consists of the `riskfortAPI` package that contains the logic for risk evaluation.

Operations that `riskfortAPI` package enables include:

- Evaluate and assess risk
- Generate advice
- List user-device associations

- Delete associations

Issuance API

RiskFort SDK (`arcot-riskfort-issuance.jar`) also consists of the `riskfortIssuanceAPI` package that enables the initial credential provisioning for users.

User management operations enabled by `Issuance` API include:

- Create user
- Update user information

Configuring Java APIs

This section provides the procedure to configure the RiskFort and Issuance Java APIs so that they can be used with the your existing application. It contains the following sections:

- Configuring Risk Evaluation Java API
- Configuring Issuance Java API

Configuring Risk Evaluation Java API

Important: Before proceeding with the configuration, ensure that the RiskFort Java API package was installed successfully during the RiskFort installation.

To configure RiskFort Risk Evaluation APIs for using with a J2EE application:

Note: The following instructions are based on Apache Tomcat Server. The configuration process might vary depending on the application server you are using. Refer to the application server documentation for detailed information on these instructions.

1. Copy the listed JAR files *from* the following location

   `<install_location>\Arcot Systems\`

   to the appropriate location in your <*APP_SERVER_HOME*> directory. For example, on Apache Tomcat this location is `<Application_Home>/WEB-INF/lib/`.

- /sdk/java/lib/arcot/**arcot_core.jar**
- /sdk/java/lib/arcot/**arcot-riskfort-evaluaterisk.jar**
- /sdk/java/lib/arcot/**arcot-riskfort-mfp.jar**
- /sdk/java/lib/arcot/**arcot-pool.jar**
- /sdk/java/lib/external/**bcprov-jdk14-139.jar**
- /sdk/java/lib/external/**commons-httpclient-3.1.jar**
- /sdk/java/lib/external/**commons-lang-2.0.jar**
- /sdk/java/lib/external/**commons-logging-1.0.4.jar**
- /sdk/java/lib/external/**commons-pool-1.4.jar**
- /sdk/java/lib/external/**json-lib-0.7.1.jar**
- /sdk/java/lib/external/**log4j-1.2.9.jar**
- /sdk/java/lib/external/**oro-2.0.8.jar**
- /sdk/java/lib/external/**xalan-2.7.0.jar**
- /sdk/java/lib/external/**xercesImpl-2.6.2.jar**
- /sdk/java/lib/external/**xml-apis-1.0.b2.jar**
- /sdk/java/lib/external/**xmlParserAPIs-2.6.2.jar**
- /sdk/java/lib/external/**xom-1.1.jar**
- /sdk/java/lib/external/**servlet-api-2.4.jar**

2. Configure the log4j.properties.risk-evaluation and riskfort.risk-evaluation.properties files:

   - If the application *already has* a configured log4j.properties.risk-evaluation file, then merge it with the following log configuration files:

     <*install_location*>/Arcot Systems\sdk\java\properties**log4j.properties.risk-evaluation**

     and

     <*install_location*>\Arcot Systems\sdk\java\properties**riskfort.risk-evaluation.properties**

   - If the application *does not have* the log4j.properties file already configured, then:

     i. Rename log4j.properties.risk-evaluation to log4j.properties.

     ii. Merge riskfort.risk-evaluation.properties with log4j.properties.

     iii. Copy the log4j.properties file to:

<*Application_Home*>/WEB-INF/classes/**properties**/

Note: To know more about APIs and their initialization, refer to the RiskFort Javadocs at <*install_location*>\Arcot Systems\docs\riskfort**Arcot-RiskFort-2.2.6-risk-evaluation-sdk-javadocs.zip**.

Configuring Issuance Java API

Important: Before proceeding with the configuration, ensure that the Issuance Java API package was installed successfully during the RiskFort installation.

To configure Issuance APIs for using with a J2EE application:

Note: The following instructions are based on Apache Tomcat Server. The configuration process might vary depending on the application server you are using. Refer to the application server documentation for detailed information on these instructions.

1. Copy the following JAR files *from* the following location *to* the appropriate location in your <*APP_SERVER_HOME*> directory:

   <*install_location*>**Arcot Systems**\

   For example, for Apache Tomcat, this location is <*Application_Home*>/WEB-INF/**lib/**.

   - /sdk/java/lib/arcot/**arcot_core.jar**
   - /sdk/java/lib/arcot/**arcot-riskfort-issuance.jar**
   - /sdk/java/lib/arcot/**arcot-pool.jar**
   - /sdk/java/lib/external/**bcprov-jdk14-139.jar**
   - /sdk/java/lib/external/**commons-beanutils-1.7.0.jar**
   - /sdk/java/lib/external/**commons-collections-3.1.jar**
   - /sdk/java/lib/external/**commons-lang-2.0.jar**
   - /sdk/java/lib/external/**commons-logging-1.0.4.jar**
   - /sdk/java/lib/external/**commons-pool-1.4.jar**
   - /sdk/java/lib/external/**dom4j-1.6.1.jar**
   - /sdk/java/lib/external/**jaxen-1.1-beta-8.jar**

- /sdk/java/lib/external/**jdom-1.0.jar**
- /sdk/java/lib/external/**log4j-1.2.9.jar**
- /sdk/java/lib/external/**oro-2.0.8.jar**
- /sdk/java/lib/external/**xalan-2.7.0.jar**
- /sdk/java/lib/external/**xercesImpl-2.6.2.jar**
- /sdk/java/lib/external/**xml-apis-1.0.b2.jar**
- /sdk/java/lib/external/**xmlParserAPIs-2.6.2.jar**
- /sdk/java/lib/external/**xom-1.1.jar**

2. Configure the log4j.properties.riskfort-issuance file:
   - If the application has an *already configured* log4j.properties file, then merge it with the following log configuration file:

     <*install_location*>\Arcot Systems\sdk\java\properties**log4j.properties.riskfort-issuance**
   - If the application *does not have* the log4j.properties file already configured, then:
     i. Rename log4j.properties.riskfort-issuance to log4j.properties.
     ii. Copy the file to:

     <*APP_SERVER_ROOT*>/WEB-INF/classes/**properties**/

Note: To know more about APIs and their initialization, refer to the Issuance Javadocs at <*install_location*>\Arcot Systems\docs\riskfort**Arcot-RiskFort-2.2.6-issuance-sdk-javadocs.zip**.

Working with RiskFort Web Services

This section guides you through the steps for:

- Generating Risk Evaluation Client Code
- Generating Issuance Client Code
- Generating Administration Client Code

Important: Before proceeding with the client code generation, as discussed in the following sub-sections, you *must* ensure that the RiskFort package was installed successfully and that the Server is up and running.

Generating Risk Evaluation Client Code

After the installation, you need to generate the client stub by using the `ArcotRiskFortEvaluateRiskSvc.wsdl` file, which enables the Web Services client to communicate with the RiskFort Server. This file is available in the following directory:

`<install_location>\Arcot Systems\wsdls\riskfort\`

The steps to generate the client stub are:

1. Stop the application server.
2. Navigate to the following location:

   `<install_location>\Arcot Systems\wsdls\riskfort\`
3. Use the `ArcotRiskFortEvaluateRiskSvc.wsdl` file to generate the client code.
4. Restart the application server.
5. In a browser window, access the following URL to verify if the client can access the Web Service:

   http://<RISKFORT_SERVER_IP>:<PORT>/services/RiskFortEvaluateRiskSvc

Note: To know more about Web Services, refer to the RiskFort WSDLdocs at `<install_location>\Arcot Systems\docs\riskfort\` **`Arcot-RiskFort-2.2.6-risk-evaluation-wsdldocs.zip`**.

Generating Issuance Client Code

After the installation, you need to generate the client stub by using the `ArcotRiskFortIssuanceSvc.wsdl` file, which enables you to generate the Issuance Web Services client code to communicate with the RiskFort Server. This file is available in the following directory:

`<install_location>\Arcot Systems\wsdls\riskfort\`

The steps to generate the client stub are:

1. Stop the application server.
2. Navigate to the following location:

   `<install_location>\Arcot Systems\wsdls\riskfort\`
3. Use the `ArcotRiskFortIssuanceSvc.wsdl` file to generate the client code.
4. Restart the application server.
5. In a browser window, access the following URL to verify if the client can access the Web Service:

   http://<RISKFORT_SERVER_IP>:<PORT>/services/RiskFortIssuanceSvc

Note: To know more about Web Services, refer to the Issuance WSDLdocs at `<install_location>\Arcot Systems\docs\riskfort\Arcot-RiskFort-2.2.6-issuance-wsdldocs.zip`.

Generating Administration Client Code

The `wsdls\admin\` directory in `ARCOT_HOME` also contains the accompanying WSDL (`ArcotRiskFortAdminWebService.wsdl`) that can be used to generate the Web Services client code to communicate with the RiskFort Web Services.

The steps to generate the client stub are:

1. Stop the application server.
2. Navigate to the following location:

   `<install_location>\Arcot Systems\wsdls\admin\`
3. Use the `ArcotRiskFortAdminWebService.wsdl` WSDL to generate the client code.
4. Restart the application server.
5. In a browser window, access the following URL to verify if the client can access the Web Service:

   http://<RISKFORT_SERVER_IP>:<PORT>/ArcotRiskFortAdminWebService/services/ArcotRiskFortAdminWebService

Note: To know more about Web services, refer to the Administration WSDLdocs at `<install_location>\Arcot Systems\docs\riskfort\Arcot-RiskFort-2.2.6-AdminWebService-wsdldocs.zip`.

Configuring Device ID

RiskFort uses Device ID to register and identify the device that is used by a user during transactions. The Device ID needs to be set as a cookie on the user computer. This cookie can either be a HTTP cookie or a Flash object.

This section discusses the configuration of these cookies. It covers the following topics:

- Configuring HTTP Cookies
- Configuring Flash Objects

Configuring HTTP Cookies

When you perform Complete installation (see "Performing Complete Installation" on page 4-44 for more information) or select to install RiskFort Evaluation SDK or Web Service in the Choose Install Set screen (see Step 5 on page 5-77 for more information), the following file is automatically installed:

`<install_location>\Arcot Systems\sdk\javascript\rfutil.js`

This file provides JavaScript functions to get and set the HTTP cookies.

HTTP Cookie Configuration

To configure for an HTTP cookie to be set on the end-user computer, you must include `rfutil.js` in your application page(s) that get or set the HTTP cookies.

To do so:

1. Copy `rfutil.js` to an appropriate Web application directory that is relative to the location where the page (in which you are including the `rfutil.js` file) is available.
2. Include the following JavaScript code in the relevant Web page of your application:

```
<script type="text/javascript" src="location_to_rfutil.js"></script>
```

   In the preceding code snippet, replace *`location_to_rfutil.js`* with the relative path to `rfutil.js`.

Configuring Flash Objects

When you perform Complete installation (see "Performing Complete Installation" on page 4-44 for more information) or select to install RiskFort Evaluation SDK or Web Service in the Choose Install Set screen (see Step 5 on page 5-77 for more information), the following files are automatically installed:

- rfutil.js
- rfdevice.swf
- crossdomain.txt

rfutil.js

This file is installed at the following location:

`<install_location>\Arcot Systems\sdk\javascript\rfutil.js`

It provides JavaScript functions to get and set the Flash objects for Device ID.

	**Important:** This file *must* be included in your application page(s) that get or set Flash objects.

rfdevice.swf

This file is installed at the following location:

`<install_location>\Arcot Systems\sdk\flash\rfdevice.swf`

It manges Flash objects and provides support for cross-domain access to the cookies, so that your application pages from one domain can access the cookies set in a different domain.

	**Important:** In the all application pages, `rfdevice.swf` *must* be referred with complete and the same URL.

crossdomain.txt

This file is installed at the following location:

`<install_location>\Arcot Systems\sdk\flash\crossdomain.txt`

It specifies the list of domains that are allowed to access the Flash object. By default only sub-domains of the domain from where the RiskFort Flash movie is served are allowed to access the Flash object.

The format of a domain entry in `crossdomain.txt` is as follows:

```
&domainName=<pipe-separated_domain_list>&
```

Important: This file *must* reside in the same location as `rfdevice.swf`.

Flash Object Configuration

To configure for a Flash object to be set on the end-user computer, perform the following steps:

1. Include `rfutil.js` in your application page(s) that get or set the Flash object.
   a. Copy `rfutil.js` to an appropriate Web application directory that is relative to the location where the page (in which you are including the `rfutil.js` file) is available.
   b. Include the following JavaScript code in the relevant Web page of your application:

   ```
   <script type="text/javascript"
   src="location_to_rfutil.js"></script>
   ```

   In the preceding code snippet, replace *`location_to_rfutil.js`* with the relative path to `rfutil.js`.
2. Copy `rfdevice.swf` and `crossdomain.txt` to the appropriate Web application directory.

Important: The `crossdomain.txt` file *must* reside in the same location as `rfdevice.swf`.

3. If your Flash object will be accessed across domains, then add the list of domains in the following format in `crossdomain.txt`:

```
&domainName=<pipe-separated_domain_list>&
```

For example, for a Web site that has aggregated pages from its own site and its partner site, the entry will be as follows:

```
&domainName=*.my-bank.com|*.my-partner.com&
```

4. Ensure that in the all application pages, `rfdevice.swf` is referred with absolute and same URL.

   For example, if `rfdevice.swf` is delivered from `login.my-bank.com`, then both sites (`login.my-bank.com` and `online.my-partner.com`) must include `rfdevice.swf` from `login.my-bank.com`.

Enabling SSL Communication

RiskFort supports Secure Socket Layer (SSL) communication between the RiskFort Server and its Java SDKs. Based on the application server you are using, see Appendix F, "Configuring SSL" for detailed information on setting SSL as the transport mode between RiskFort Server and its clients.

Chapter 7
Uninstalling RiskFort

Before you uninstall RiskFort, you must first remove its schema and then proceed with the uninstallation process. You can either use the **Add/Remove Programs** utility in the Microsoft Windows Control Panel to uninstall RiskFort or run the uninstaller file (`Uninstall Arcot RiskFort.exe`) to remove RiskFort from your system. After you complete the uninstallation, you must then perform the post-uninstallation tasks to clean up the residual WAR files and entries.

This chapter guides you through the steps for uninstalling RiskFort and its components. The chapter covers the following sections:

Dropping RiskFort Schema

Note: If for some reason, you need to retain the database, then *do not* proceed with the instructions in this section.
Refer to section "Uninstalling RiskFort Server" to proceed with the uninstallation.

To uninstall the RiskFort database:

1. Navigate to the following directory:

   `<install_location>\Arcot Systems\`**`dbscripts`**`\`

2. Based on the database you are using, navigate to one of the following subdirectories:
   - **For Oracle:**

     `<install_location>\Arcot Systems\dbscripts\`**`oracle`**`\`
   - **For MS SQL:**

     `<install_location>\Arcot Systems\dbscripts\`**`mssql`**`\`

3. Run the scripts in the *following* order to drop all database tables of RiskFort and related components:
   - `drop-riskfort-2.2.6.sql`
   - `drop-arcot-common-1.0.sql`

Uninstalling RiskFort Server

To uninstall RiskFort Server:

1. Shut down the following gracefully:
   a. RiskFort Server
   b. Any application servers where other RiskFort components are deployed
2. Close the Administration Console, if open.
3. Ensure that all INI and other RiskFort files are closed.
4. On the desktop, click **Start, Settings**, **Control Panel, Add/Remove Programs** to open the Add or Remove Programs window.
5. From the **Currently installed programs** list, select **Arcot RiskFort**, and click **Change/Remove.**

   The Uninstall Arcot RiskFort window appears.

Note: You can also uninstall RiskFort by running `Uninstall Arcot RiskFort.exe` in the `<install_location>\Arcot Systems\Uninstall Arcot RiskFort` directory.

6. In the wizard window:
   - Select **Complete Uninstall** to uninstall *all* components of RiskFort and go to Step 8.

Note: You might have to wait for a few minutes for the uninstalltion to complete.

   - Select **Uninstall Specific Features** to uninstall the selected components, and click **Next** to display the Choose Product Features screen.

This screen displays the RiskFort components that are installed on the system. Go to Step 7.

7. Deselect the components you wish to uninstall and click **Uninstall** to display the Uninstall Arcot RiskFort window.

Note: You might have to wait for a few minutes for the uninstalltion to complete.

After the software is uninstalled successfully, the *Uninstallation Complete* screen appears with a success message.

8. Click **Yes, restart my system** to restart the computer immediately or **No, I'll restart my system later** to restart the computer later, as required.

Note: RiskFort or its components that you selected to uninstall will be completely removed only *after* the computer has been restarted.

9. Click **Done** to exit the wizard and complete the uninstallation.

Performing Post-Uninstallation Tasks

The post-uninstallation steps that you need to perform to ensure that all RiskFort components are removed are:

1. Delete the `<install_location>\Arcot Systems\` directory, if not required after uninstallation.

Note: If multiple Arcot products are installed on this system, then delete this directory *only if* RiskFort is the last product to be uninstalled.

2. Uninstall the following WAR files from the appropriate sub-directory in *<APP-SERVER-HOME>*.

Note: Here, *APP-SERVER-HOME* represents the directory path where application server (for example, Apache Tomcat) is installed.

Refer to the Application server vendor documentation for detailed information on uninstalling the WAR files.

- `arcotadmin.war`: Administration Console
- `arcotuds.war`: User Data Service
- `riskfort-2.2.6-sample-application.war`: Sample Application
- `riskfort-2.2.6-sample-callouts.war`: Sample Callout

Note: If you have a distributed-system deployment, then locate these files on the system where you have deployed the particular application.

3. If Oracle Database was used for database setup, then delete the `tabspace_arreports_<time_database_was_created>.dat` file from the system running the RiskFort database.
4. Delete the DSN entry created during the RiskFort installation.

   To delete this entry, open the Control Panel, navigate to **Administrative Tools, Data Sources (ODBC), System DSN**, select the required DSN, and click **Remove.**

Appendix A
RiskFort Directory Structure

This appendix provides the information about the location of all files that are installed by the RiskFort installer. It covers:

- RiskFort Directory Structure
- RiskFort Issuance SDK Files
- RiskFort Risk Evaluation SDK Files
- RiskFort WSDL Files

RiskFort Directory Structure

Table A-1 lists the main directories, files, and JARs that are created by the RiskFort installer. It also describes specific subdirectories and files that have been referred to in this manual.

Note: In addition to the files and directories discussed in the table, you will also see a blank file called `arcotkey` in the `Arcot Systems` directory. This file is used by the installer to detect previously installed Arcot products. If you delete this file, then the installer will not be able to detect previously installed Arcot products, and will allow new installations to be performed in any location. As a result, the installer will not be able to ensure the same destination directory for multiple Arcot products and components, in which case, the products (or components) might not work, as expected. This file has no impact on patches and upgrade.

Table A-1. Installation Directory Structure for Windows

Directory	Used By	File Names and Description
`<install_location>\Arcot Systems\bin\` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more details on these tools.	• RiskFort Server • Case Management Queuing Server	Contains the following executable files used by RiskFort Server: • `arrfadmin.exe` (Tool for refreshing and gracefully shutting down the RiskFort Server.) • `arrfcasemgmtserver.exe` (Tool for refreshing and gracefully shutting down the Case Management Queuing Server module.) • `arrfserver.exe` (Tool for setting the server management port and other server-related operations.) • `arrfupload.exe` (Tool for uploading Quova data to RiskFort database.) • `arrfversion.exe` (Tool for determining the version of the modules provided by Arcot.) • `DBUtil.exe` (Tool for editing the `securestore.enc` file that stores encrypted information needed to connect to the RiskFort database.) Also contains the following library files used by RiskFort Server: • `aradminprotocol.dll` • `aradminwsprotocol.dll` • `arRiskEngine.dll` • `NameValueXref.dll` • `transwsprotocol.dll`

Table A-1. Installation Directory Structure for Windows

Directory	Used By	File Names and Description
	• User Data Service (UDS) • Administration Console	• `DBUtil.exe` (Tool for editing the `securestore.enc` file that stores encrypted information needed to connect to the RiskFort database.)
`<install_location>\Arcot Systems\`**`conf`**`\` See Appendix B, "Configuration Files and Options" for more details on the configuration files that you see in this directory.	• Administration Console	Contains the following configuration files for use by the Administration Console: • `adminserver.ini` • `application.xml` (Required for creating EAR files for the Administration Console) • `arcotcommon.ini`
	• RiskFort Server	Contains the following configuration files for use by RiskFort Server and other RiskFort components: • `arcotcommon.ini` • `riskfortadminclient.ini` • `riskfortcasemgmtserver.ini` • `riskfortdataupload.ini` • `riskfortserver.ini` • `securestore.enc`
	• UDS	Contains the following configuration files for use by UDS: • `udsserver.ini` • `application.xml` (Required for creating EAR files for UDS)
`<install_location>\Arcot Systems\`**`dbscripts`**`\`	• Administration Console • RiskFort Server • UDS	Contains the database scripts to create and drop RiskFort schemas for the Database Type (**Oracle** or **MS SQL**) that you specified during installation.

Table A-1. Installation Directory Structure for Windows

Directory	Used By	File Names and Description
`<install_location>\Arcot Systems\docs\riskfort\`	• RiskFort Server	Contains the following zips and XSDs for writing Callouts, and the Javadocs and WSDLdocs for Risk Evaluation and Issuance SDKs: • `Arcot-RiskFort-2.2.6-CallOutInterface-xsds.zip` (The Evaluation and Scoring Request and Response files required for writing a Callout.) • `Arcot-RiskFort-2.2.6-issuance-sdk-javadocs.zip` • `Arcot-RiskFort-2.2.6-issuance-wsdldocs.zip` • `Arcot-RiskFort-2.2.6-risk-evaluation-wsdldocs.zip` • `Arcot-RiskFort-2.2.6-risk-evaluation-sdk-javadocs.zip`
	• Administration Console	Contains the following zipped WSDLdocs for corresponding Administration SDKs: • `Arcot-RiskFort-2.2.6-AdminWebService-wsdldocs.zip` (The WAR file required to deploy the `Admin` Web Service.)
`<install_location>\Arcot Systems\java\ext\`	• Administration Console • UDS	The **`ext`** subdirectory contains the following files (in appropriate subdirectories) used to read the contents of `securestore.enc` for your OS platform: • `arcot-crypto-util.jar` • `ArcotAccessKeyProvider.dll`
`<install_location>\Arcot Systems\java\lib\`		The **`lib`** subdirectory contains the WAR file required by the Administration Console Framework: • `adminframework.war`

Table A-1. Installation Directory Structure for Windows

Directory	Used By	File Names and Description
`<install_location>\Arcot Systems\java\webapps\`	• Administration Console	Contains the following WAR files required by the Administration Console: • `arcotadmin.war` (The WAR file required to deploy the Administration Console.)
	• UDS	Contains the WAR file required by UDS: • `arcotuds.war` (The WAR file required to deploy UDS.)
`<install_location>\Arcot Systems\logs\`	• Administration Console • RiskFort Server • Case Management Queuing Server • UDS	Contains the latest installation and other log files used by Administration Console, RiskFort, and UDS: • `Arcot_RiskFort_InstallLog.log` • `arcotadmin.log` • `arcotriskfort.log` • `arcotriskfortcasemgmtserver.log` • `arcotuds.log` The **`backup`** subdirectory contains the older logs. **Book:** See Appendix A, "RiskFort Logging" in the *Arcot RiskFort 2.2.6 Administration Guide* for detailed information on these log files.

Table A-1. Installation Directory Structure for Windows

Directory	Used By	File Names and Description
`<install_location>\Arcot Systems\`**`plugins\rules\`**	• RiskFort Server	Contains all the DLL (library binary) files to support all the out-of-box Riskfort rules and Scoring. • The **`addon\`** directory contains the DLL files for the Add-On rules shipped with the release. **Important:** The `addon\` directory *must* also contain the DLL files, if you deploy one or more of your custom rules.
`<install_location>\Arcot Systems\`**`resourcepacks\`**	• Administration Console • UDS	Contains the following Administration Console pack bundles required by the Administration Console Framework and UDS: • `bundler_adminconsole.zip` • `bundle_riskfort.zip`

`<install_location>\Arcot Systems\`**`samples\java\`**	• RiskFort Server
	• RiskFort Issuance SDK
	• RiskFort Risk Evaluation SDK
		Contains the following subdirectories:
		• The **`addonruletype`** subdirectory contains the sample XML file that you can use to define a custom rule type and its parameters.
		Book: See the *Arcot RiskFort 2.2.6 Administration Guide* for more information on Add-On rules and how to deploy these rules.
		• The **`java`** subdirectory contains the WAR files for:
		  • `riskfort-2.2.6-sample-application.war` to deploy the RiskFort Sample Application.
		  • `riskfort-2.2.6-sample-callouts.war` to deploy the RiskFort Sample Callout.

Table A-1. Installation Directory Structure for Windows

Directory	Used By	File Names and Description
<install_location>\Arcot Systems**sdk**\	• RiskFort Issuance SDK • RiskFort Risk Evaluation SDK	Contains SDKs and dependant files supported by RiskFort in the **c**, **flash**, and **java** flavors. The **javascript** subdirectory contains the accompanying JavaScripts that are used by these SDKs and the DeviceDNA module. See sections "RiskFort Issuance SDK Files" and "RiskFort Risk Evaluation SDK Files" later in this appendix for detailed explanation of the contents of this directory.
<install_location>\Arcot Systems**tools****bundlemanager**\	• Administration Console	Contains the files required by the Administration Console Resourcepack.

<install_location>\Arcot Systems**Uninstall_Arcot RiskFort**\	• RiskFort Server	Contains the files required to uninstall RiskFort. In addition:
		• The **jre** subdirectory contains all files required for Java Runtime Environment (JRE) support:
		  • Java Virtual Machine
		  • Runtime Class Libraries
		  • Java Application Launcher
		• The **resource** directory contains all files required by the installer for uninstallation of RiskFort.

<install_location>\Arcot Systems **wsdls**\	• RiskFort Server	Contains the WSDL files required by the Administration Console (the **admin** subdirectory) and RiskFort (the **riskfort** subdirectory.) See section, "RiskFort Risk Evaluation SDK Files" later in this appendix for detailed explanation of the contents of this directory.

RiskFort Issuance SDK Files

Table A-2 lists the directory location of the files that are used by Issuance SDK.

Table A-2. Issuance SDK Files

Directory	File Description
<*install_location*>\Arcot Systems**docs****riskfort**\	Contains the Arcot-RiskFort-2.2.6-issuance-sdk-javadocs.zip file, which contains the Javadocs for Issuance SDK.
<*install_location*>\Arcot Systems**samples****java**\	Contains the riskfort-2.2.6-sample-application.war file to deploy Sample Application.
<*install_location*>\Arcot Systems**sdk**\	Contains SDKs and dependant files supported by RiskFort.
<*install_location*>\Arcot Systems**sdk****java**\	• The **lib** subdirectory contains the Arcot-supplied and third-party JAR files. • The **properties** directory contains the property files required for configuration of RiskFort.
<*install_location*>\Arcot Systems**sdk****java****lib****arcot**\	Contains the following Arcot JAR files used by Issuance Java SDK. • arcot_core.jar • arcot-pool.jar • arcot-riskfort-issuance.jar

Table A-2. Issuance SDK Files

Directory	File Description
<install_location>\Arcot Systems**sdk\java\lib\external**\	Contains the third-party JAR files required by RiskFort Issuance Java SDK. • bcprov-jdk14-139.jar • commons-beanutils-1.7.0.jar • commons-collections-3.1.jar • commons-httpclient-3.1.jar • commons-lang-2.0.jar • commons-logging-1.0.4.jar • commons-pool-1.4.jar • dom4j-1.6.1.jar • jaxen-1.1-beta-8.jar • jdom-1.0.jar • log4j-1.2.9.jar • oro-2.0.8.jar • servlet-api-2.4.jar • xalan-2.7.0.jar • xercesImpl-2.6.2.jar • xml-apis-1.0.b2.jar • xmlParserAPIs-2.6.2.jar • xom-1.1.jar
<install_location>\Arcot Systems**sdk\java\properties**\	Contains the following files: • log4j.properties.riskfort-issuance • riskfort.issuance.properties

RiskFort Risk Evaluation SDK Files

Table A-3 lists the directory location of the files that are used by Risk Evaluation Java SDK.

Table A-3. Risk Evaluation SDK Files

Directory	File Description
<*install_location*>\Arcot Systems**docs****riskfort**\	Contains the Arcot-RiskFort-2.2.6-risk-evaluation-sdk-javadocs.zip file, which contains the Javadocs for Risk Evaluation SDK.
<*install_location*>\Arcot Systems**samples****java**\	Contains the following: riskfort-2.2.6-sample-application.war to deploy the RiskFort Sample Application. riskfort-2.2.6-sample-callouts.war to deploy the RiskFort Sample Callout Server.
<*install_location*>\Arcot Systems**sdk**\	Contains SDKs and dependant files supported by RiskFort.
<*install_location*>\Arcot Systems**sdk****flash**\	The directory contains: • crossdomain.txt, which specifies the list of domains that can access the Flash object. • rfdevice.swf, which manages the Device ID Flash object.
<*install_location*>\Arcot Systems**sdk****java**\	• The **lib** subdirectory contains the Arcot-supplied and third-party JAR files. • The **properties** directory contains the property files required for configuration of RiskFort.
<*install_location*>\Arcot Systems**sdk****java****lib****arcot**\	Contains the following Arcot JAR files used by Issuance Java SDK. • arcot_core.jar • arcot-pool.jar • arcot-riskfort-evaluaterisk.jar • arcot-riskfort-mfp.jar

Table A-3. Risk Evaluation SDK Files

Directory	File Description
<install_location>\Arcot Systems**sdk\java\lib\external**\	Contains the third-party JAR files required by RiskFort Issuance Java SDK. • bcprov-jdk14-139.jar • commons-beanutils-1.7.0.jar • commons-collections-3.1.jar • commons-httpclient-3.1.jar • commons-lang-2.0.jar • commons-logging-1.0.4.jar • commons-pool-1.4.jar • dom4j-1.6.1.jar • jaxen-1.1-beta-8.jar • jdom-1.0.jar • log4j-1.2.9.jar • oro-2.0.8.jar • servlet-api-2.4.jar • xalan-2.7.0.jar • xercesImpl-2.6.2.jar • xml-apis-1.0.b2.jar • xmlParserAPIs-2.6.2.jar • xom-1.1.jar

Table A-3. Risk Evaluation SDK Files

Directory	File Description
<*install_location*>\Arcot Systems**sdk****java****properties**\	Contains the following files: • log4j.properties.risk-evaluation • riskfort.risk-evaluation.properties
<*install_location*>\Arcot Systems**sdk****javascript**\	Contains: • ArcotDeviceDNA.js, which is required at the client-end for collecting DeviceDNA information. • deployJava.js, which is required to detect the deployed Java components at the end-user system. • FlashDetect.js, which is required to detect the deployed Adobe Flash version at the end-user system. • json.js, which is required at the client-end for collecting DeviceDNA information. • PluginDetect.js, which is required to detect the deployed plug-ins at the end-user system. • rfutil.js, which is required to get and set Flash object and load rfdevice.swf in the flash directory. • swfobject.js, which is required to detect the deployed Flash content (accessible to browsers) at the end-user system.

RiskFort WSDL Files

Table A-4 lists the directory location of the files that are used by Risk Evaluation and Issuance WSDLs.

Table A-4. RiskFort WSDL Files

Directory	File Description
`<install_location>\Arcot Systems\docs\riskfort\`	Contains the zipped WSDLdocs for RiskFort Risk Evaluation and Issuance: • `Arcot-RiskFort-2.2.6-issuance-wsdldocs.zip` • `Arcot-RiskFort-2.2.6-risk-evaluation-wsdldocs.zip` • `Arcot-RiskFort-2.2.6-AdminWebService-wsdldocs.zip`
`<install_location>\Arcot Systems\wsdls\admin\`	Contains the `ArcotRiskFortAdminWebService.wsdl` file required by the Administration Console. This WSDLdoc describes the Administration Web Services and how to access them. In addition, it can be used to add Exception Users.
`<install_location>\Arcot Systems\wsdls\riskfort\`	Contains the WSDL and XML Schema files required by RiskFort: • `ArcotRiskFortEvaluateRiskSvc.wsdl` (The WSDLdoc describes the Risk Evaluation Web Service and how to access it.) • `ArcotRiskFortIssuanceSvc.wsdl` (The WSDLdoc that describes the Issuance Web Services and how to access it.)

Appendix B
Configuration Files and Options

This appendix discusses the configuration files that RiskFort uses and the parameters that you must configure in these files. It also includes samples of these default configuration files.

The configuration files important for RiskFort can be categorized as:

- INI Files
- Properties Files

INI Files

The plain-text INI files used for configuring RiskFort include:

- adminserver.ini
- arcotcommon.ini
- riskfortadminclient.ini
- riskfortcasemgmtserver.ini
- riskfortdataupload.ini
- riskfortserver.ini
- udsserver.ini

All RiskFort configuration files are available at the following default location:

`<install_location>\Arcot Systems\conf\`

adminserver.ini

The `adminserver.ini` file contains the parameters to set the Administration Console log information. Table B-1 lists the log file information used by the Administration Console.

Table B-1. Parameters for Administration Console Configuration

Parameter	Default Value	Description
`log4j.logger.com.arcot.DEFAULT`	`INFO, roothandle` **Important:** `roothandle` is the name of the UDS log handle and *must* be specified.	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.
`log4j.logger.com.arcot.admin`	`INFO, roothandle` **Important:** `roothandle` is the name of the UDS log handle and *must* be specified.	Specify the log level that must be used to write the logs. The supported log levels are: • *`FATAL`* • *`WARNING`* • *`INFO`* • *`DEBUG`* **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.
`log4j.logger.com.arcot.admin.framework`	`INFO`	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.

Table B-1. Parameters for Administration Console Configuration

Parameter	Default Value	Description
`log4j.logger.com.arcot.adminconsole`	`INFO, roothandle` **Important:** `roothandle` is the name of the Administration Console log handle and *must* be specified.	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.
`log4j.logger.com.arcot.database`	`INFO, roothandle` **Important:** `roothandle` is the name of the log handle for the database used by the Administration Console and *must* be specified.	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.
`log4j.logger.com.arcot.common.database`	`INFO, dbfohandle` **Important:** `dbfohandle` is the name of the database failover log handle and *must* be specified.	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.

Table B-1. Parameters for Administration Console Configuration

Parameter	Default Value	Description
log4j.appender.debuglog.File	${arcot.home}/logs/**arcotadmin.log**	The log file name and the location where the Administration Console logs will be created. By default, the Administration Console log file name is arcotadmin.log and is created in the following location: <*install_location*>\Arcot Systems**logs**\
log4j.appender.debuglog.MaxFileSize	10 MB	The maximum allowed file size of the log file.
log4j.appender.debuglog.MaxBackupIndex	100	The maximum number of backup files that can be created. When the number of backup files reaches this number, then the application starts to overwrite from the first log file.

arcotcommon.ini

The arcotcommon.ini file contains the parameters for database and instance settings for RiskFort Sever and other components (Administration Console and User Data Service) of RiskFort. Typically, you will need to edit the following sections in this file:

- Database Settings
- Instance Settings

Database Settings

The database settings in arcotcommon.ini allow you to identify the database to which the server will be connected and the backup database to use for failover. These settings also enable you to configure database communications resources available between the server and the database.

Note: For notes and recommendations for database settings, refer to the "Configuring Database Server" section in Chapter 3, "Preparing for Installation".

You must edit the following sections related to database settings in the arcotcommon.ini file:

- [arcot/db/dbconfig]
- [arcot/db/primarydb]
- [arcot/db/backupdb]

[arcot/db/dbconfig]

This section enables you to specify the type of the database (Oracle or MS-SQL) and generic information about this database type. Table B-2 lists the database setting parameters in `[arcot/db/dbconfig]` section.

Table B-2. Database Setting Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
`DbType`	`--`	The type of the database applicable to all database connections. The supported values are: • `oracle` • `mssqlserver`
`Driver`	`--`	The fully-qualified name of the database driver class that is supplied by the JDBC driver vendor. **Note:** Consult your JDBC vendor documentation for the right driver name. For example: • **Oracle:** `oracle.jdbc.driver.OracleDriver` • **MSSQL Server:** `com.microsoft.sqlserver.jdbc.SQLServerDriver`
`MinConnections`	`4`	The minimum number of connections to initially create between the server and the database.
`MaxConnections`	`32`	The maximum number of connections that will be created between the server and the database. **Note:** There is a limit to how many connections a database will allow and that limit may limit the server from creating `MaxConnections` number of connections. See your database driver documentation for more information about the limit on number of inbound connections.

Table B-2. Database Setting Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
IncConnections	2	The number of connections that will be created when a new connection is needed between the RiskFort components and the database.
MaxIdleConnections	4	The maximum number of idle database connections that the server can maintain.
MaxWaitTimeFor Connection	30000	The maximum time (in **milliseconds**) the server must wait for a connection to become available (when there are no available connections) before timing out.
AutoRevert	1	Whether or not the system will attempt to connect to the primary database after a failover occurs. Set AutoRevert=1, if you have a backup database configured or if you want the server to try to connect to the database after a failover occurs.
MaxTries	3	The number of times the server will attempt to connect to the database before aborting the connection.
ConnRetrySleep Time	100	The number of **milliseconds** to delay between attempts to connect to the database.
MonitorSleepTime	50	The amount of time in **seconds** the Monitoring Thread sleeps between heartbeats checks on all databases.
Profiling	0	Whether the database messages are being logged. Set the value to 1 if you want to enable logging of database messages.
EnableBrandLicensing	0	Whether a branded ODBC driver is in use.
BrandLicenseFile	IVWF.LIC	The license file name when you use a branded ODBC driver. This parameter is required if the value of EnableBrandLicensing is 1. Otherwise it is ignored. **Important:** If present, this value must *not* be edited.
MaxTransactionRetries	3	The maximum number of times the transaction is retried with a database instance for pre-defined error conditions.
TransactionRetrySleep Time	10	The interval in **milliseconds** between two consecutive transaction retries.

[arcot/db/primarydb]

This section enables you to specify the primary database to which the RiskFort Server will be connected. You can configure more than one primary databases by specifying the required number, *N* in the following parameters:

- `Datasource.<N>`
- `AppServerConnectionPoolName.<N>`
- `Username.<N>`
- `URL.<N>`

Table B-3 lists the database setting parameters in the `[arcot/db/primarydb]` section.

Table B-3. Primary Database Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
`Datasource.<N>`	No default	The name of the ODBC System Data Source Name (DSN) pointing to the primary database hosting the server data.
`AppServerConnection PoolName.<N>`	No default	The JNDI name used to look up the connection pool object, if the database connection pooling feature of the application server is being used. A pool by this JNDI name should be created in the containing application server, and sufficient access right must be given to Arcot Web applications for it to use the connection pool: • If the JNDI name is configured in **Apache Tomcat**, then use a fully qualified JNDI name. For example: • `AppServerConnectionPoolName.1=java:comp/env/SampleDS` • For **other application servers**, specify only the JNDI name. For example: • `AppServerConnectionPoolName.1=SampleDS` See Appendix E, “Configuring Application Server for Database Connection Pooling” for more information. If the application server connection pool is *not* required, then leave this configuration empty.

Table B-3. Primary Database Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
`URL.<N>`	No default	The name of the JDBC data source. For • **Oracle** -> `jdbc:oracle:thin:<server>:<port>:<sid>` • **MS SQLServer** -> `jdbc:sqlserver://<server>:<port>;databaseName=<databasename>;selectMethod=cursor`
`Username.<N>`	No default	The user ID used by the server to access the database.
`TrustStorePath`	No default	The SSL Certificate Truststore Path corresponding to `Datasource.<N>`. The path (including the filename) refers to the certificate Trust Store file, which contains the list of certificates that the client trusts. **Important:** The password corresponding to `TrustStorePath.<N>` must be securely stored in `securestore.enc`, with the value of `TrustStorePath.<N>` as the key. The `dbutil` utility is used to achieve this. **Book:** See the *Arcot RiskFort 2.2.6 Administration Guide* for more information on `dbutil`.
`HostNameInCertificate.<N>`	No default	The value of Common Name (CN) in the subject Distinguished Name (DN) of `Datasource.<N>` SSL Certificate in Truststore.

[arcot/db/backupdb]

This section `[arcot/db/backupdb]` enables you to specify the backup database to use for failover. You can configure more than one failover databases by specifying the required number, *N* in the following parameters:

- `Datasource.<N>`
- `AppServerConnectionPoolName.<N>`
- `Username.<N>`
- `URL.<N>`
- `TrustStorePath`

- `HostNameInCertificate.<N>`

This section uses the same parameters as the [arcot/db/primarydb] section. Refer to Table B-3 for the list of the database setting parameters in this section.

Instance Settings

In a farm of servers, it is recommended that every instance of the server has its own unique identification. RiskFort supports a parameter to set and identify every instance of the servers. This section enables you to configure these system-wide settings for unique instances. Table B-4 lists the instance setting parameters in the `[arcot/system]` section.

Table B-4. Instance Parameter in the `[arcot/system]` Section

Parameter	Default	Description
`InstanceId`	1	The parameter that can be used to identify any server instance. It is recommended that you provide unique values for every instance of the server. The server instance is also displayed in the transaction reports, making it easier to trace the server instance to the transaction.

riskfortadminclient.ini

The `riskfortadminclient.ini` file helps the **`arrfadmin`** system administration tool (which is available in the `bin` directory of the `ARCOT_HOME` after RiskFort installation) establish two-way SSL connection between itself and the RiskFort Server.

The `riskfortadminclient.ini` file is available at the following location:

`<install_location>\Arcot Systems\conf\`

Table B-5 lists the parameters in the file.

Table B-5. Parameters in `riskfortadminclient.ini` File

Parameter	Default	Description
`Host`	`localhost`	The host name or the IP Address of the system where RiskFort Server is running.
`Port`	`7980`	The port number on which server is listening to server management requests.

Table B-5. Parameters in `riskfortadminclient.ini` File

Parameter	Default	Description
`Transport`	`tcp`	The transport mode for server management listener. The possible values are: • `TCP` • `SSL`
`SSLClientKey`	No Default	The absolute path of the base64-encoded (PEM formatted) SSL key to be used by the `arrrfadmin` tool, if two-way SSL communication is required between the tool and the RiskFort Server.
`SSLClientCertChain`	No Default	The absolute path of the base64-encoded (PEM formatted) SSL certificate or certificate chain to be used by the `arrrfadmin` tool, if two-way SSL communication is required between the tool and the RiskFort Server.
`SSLServerCACert`	No Default	The absolute path of the base64-encoded (PEM formatted) SSL CA certificate that the `arrrfadmin` tool must trust during the SSL communication between the tool and the RiskFort Server.

riskfortcasemgmtserver.ini

By using the `riskfortcasemgmtserver.ini` file, you can configure the following settings for the Case Management module of RiskFort:

- Log File Settings
- Case Management Queuing Server Settings

Log File Settings

The RiskFort Case Management Queuing Server module records all actions related to Case Management in the `arcotriskfortcasemgmtserver.log` file. The default location of this file is:

`<install_location>\Arcot Systems\logs\`

You can define a log file name for your servers log file in the INI files. You can also define the maximum file size of the primary log file. Once the primary log file reaches the maximum size, the system will then record new actions in a new primary log file (in other words, in a new instance of `arcotriskfortcasemgmtserver.log`.)

All logging related parameters are under the section `[arcot/riskfortcasemgmtserver/logger]` in the `arcotriskfortcasemgmtserver.ini` file. Table B-6 lists the log file setting parameters in the `riskfortserver.ini` files and provides descriptions of each:

Table B-6. Log File Parameters in `riskfortcasemgmtserver.ini`

Parameter	Default	Description
`LogFile`	`logs/arcotriskfortcasemgmtserver.log`	The file path to the default directory and the file name of the log file. **Note:** This path is relative to `ARCOT_HOME` (`<install_location>\Arcot Systems\`).
`LogFileSize`	10485760	The maximum number of **bytes** the log file can contain. When a log file reaches this size, a new file is started 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` (`<install_location>\Arcot Systems\`).
`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`
`LogTimeGMT`	0	The parameter which indicates the time zone of the time stamp in the log files. The possible values are: • `0 Local Time` • `1 GMT`

Case Management Queuing Server Settings

The thread settings for the Case Management, as shown in Table B-7, can be found under the `[arcot/riskfortcasemgmtserver/server]` section in the `riskfortcasemgmtserver.ini` file. If these entries are removed or commented, then the Case Management Queuing Server defaults to infinite wait.

Table B-7. Case Management Queuing Server Configuration Setting Parameters

Parameter	Default	Description
`MaxThreads`	128	The maximum number of threads that this Server module can maintain for serving Case Management calls at any time. **Note:** This directly impacts the number of concurrent requests the server can process.
`MinThreads`	32	The minimum number of threads that this Server module must maintain for serving Case Management calls at any time.
`ReadTimeout`	7200000	Maximum time in **milliseconds** that the Case Management Queuing Server waits for a response before closing a connection.

riskfortdataupload.ini

RiskFort uses Quova data to identify the geolocation of a user by using the IP address of the system from which the transaction originated. It then uses this data to evaluate Negative Country, Negative IP, and Zone Hopping rules.

RiskFort is shipped with the *Arcot RiskFort Data Upload Tool* (`arrfupload`) to enable you to upload the geolocation data from Quova files to the RiskFort database. The `riskfortdataupload.ini` file controls the behavior of the Arcot RiskFort Data Upload tool and is available at the following location:

`<install_location>\Arcot Systems\conf\`

Table B-8 lists the configuration parameters in this file.

Table B-8. Configuration Parameters for riskfortdataupload.ini

Parameter	Default	Description
Tables	Do Not Load	The tables that the user can work with. Possible values are: • GeoPoint • Anonymizer
Load	0	The indicator whether to upload the data to the table or not. Possible values are: • 0 (Do not load) • 1 (Load)
Swap	0	The indicator whether to swap the tables or not. Possible values are: • 0 (Do not swap) • 1 (Swap)
Filename	--	The name of the file from which the Quova data has to be loaded. **Important:** You must mention the absolute path to the file, along with the file name.

Note: If both, Load and Swap are set to 1, then first the table is loaded and then is swapped.

riskfortserver.ini

By using the riskfortserver.ini file, you can configure the following settings:

- Log File Settings ([arcot/riskfort/logger])
- Thread Settings ([arcot/riskfort/server])
- Other Server Settings

Log File Settings ([arcot/riskfort/logger])

RiskFort records all system actions in the `arcotriskfort.log` file. The default location of this file is:

`<install_location>\Arcot Systems\logs\`

You can define a log file name for your servers log file in the INI files. You can also define the maximum file size of the primary log file. Once the primary log file reaches the maximum size, the system will then record new actions in a new primary log file (in other words, in a new instance of `arcotriskfort.log`.)

All logging related parameters are under the section `[arcot/riskfort/logger]` in the `riskfortserver.ini` file. Table B-9 lists the log file setting parameters in the `riskfortserver.ini` files and provides descriptions of each:

Table B-9. Log File Parameters in `riskfortserver.ini`

Parameter	Default	Description
`LogFile`	`logs/arcotriskfort.log`	The file path to the default directory and the file name of the log file. **Note:** This path is relative to `ARCOT_HOME` (`<install_location>\Arcot Systems\`).
`LogFileSize`	10485760	The maximum number of **bytes** the log file can contain. When a log file reaches this size, a new file is started 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` (`<install_location>\Arcot Systems\`).

Table B-9. Log File Parameters in `riskfortserver.ini`

Parameter	Default	Description
`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`
`LogTimeGMT`	0	The parameter which indicates the time zone of the time stamp in the log files. The possible values are: • `0 Local Time` • `1 GMT`

Thread Settings ([arcot/riskfort/server])

A *thread* is a single sequential flow of control within a program, similar to a process (or running a program) but easier to create and destroy than a process because less resource management is involved. Each thread must have its own resources. In a multi-threaded environment, multiple threads can be spawned and operate simultaneously. This allows the system to share a single environment for all of the threads, reducing the overhead of each individual thread.

There are three factors to consider when determining the maximum and minimum number of threads that will be available for the system:

1. Each thread uses a certain amount of resources and decreases the overall performance of the system.
2. Opening and closing a thread takes up to three times the resources that are required to maintain an open thread.
3. Based on the server's capacity, there is a maximum number of threads that can be opened simultaneously before the server's performance drops below acceptable levels.

The trick is to set the minimum number of threads to handle average system use levels. Set the maximum number of threads at a level high enough to handle any peak load that the system may encounter while maintaining acceptable server performance.

The thread settings for RiskFort can be found under the `[arcot/riskfort/server]` section in the `riskfortserver.ini` file. Table B-10 lists the thread setting parameters in the `ini` files and provides descriptions of each:

Table B-10. Thread Setting Parameters

Parameter	Default	Description
`MaxThreads`	128	The maximum number of threads that the RiskFort Server can maintain for serving Risk Evaluation and Issuance calls at any time. **Note:** This directly impacts the number of concurrent requests the server can process.
`MinThreads`	32	The minimum number of threads that the RiskFort Server must maintain for serving Risk Evaluation and Issuance calls at any time.
`MaxTransWSThreads`	128	The maximum number of threads that the Issuance and Risk Evaluation Web services can maintain.
`MinTransWSThreads`	32	The minimum number of threads that the Issuance and Risk Evaluation Web services must maintain at all times.
`MaxAdminWSThreads`	32	The maximum number of threads that the Administration Web service can maintain.
`MinAdminWSThreads`	16	The minimum number of threads that the Administration Web service must maintain at all times.

Other Server Settings

The other Server configuration settings, as shown in Table B-11, can be found under the `[arcot/riskfort/server]` section in the `riskfortserver.ini` file. If these entries are removed or commented, then RiskFort Server defaults to infinite wait.

Table B-11. Server Configuration Setting Parameters

Parameter	Default	Description
`ReadTimeout`	7200000	Maximum time in **milliseconds** that the Issuance and Risk Evaluation APIs wait for a response from the RiskFort Server.
`ReadTimeoutTransWS`	7200000	Maximum time in **milliseconds** that the Issuance and Risk Evaluation Web services wait for a response from the RiskFort Server.
`ReadTimeoutAdminWS`	7200000	Maximum time in **milliseconds** that the Administration Web service waits for a response from the RiskFort Server.

udsserver.ini

The `udsserver.ini` file contains the parameters to set the User Data Service (UDS) log information. Table B-12 provides information on parameters that you need to configure for RiskFort.

Table B-12. Parameters for UDS and Database Failover Configuration

Parameter	Default Value	Description
`log4j.logger.com.arcot.uds`	`INFO, debuglog` **Important:** `debuglog` is the name of the UDS log handle and *must* be specified.	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.
`log4j.logger.com.arcot.common.database`	`INFO, dbfohandle` **Important:** `dbfohandle` is the name of the database failover log handle and *must* be specified.	
`log4j.appender.debuglog.File`	`${arcot.home}/logs/arcotuds.log`	The log file name and the location where the UDS logs will be created. By default, the UDS log file name is `arcotuds.log` and is created in the following location: `<install_location>\Arcot Systems\logs\`
`log4j.appender.debuglog.MaxFileSize`	10 MB	The maximum allowed file size of the log file.
`log4j.appender.debuglog.MaxBackupIndex`	100	The maximum number of backup files that can be created. When the number of backup files reaches this number, then the application starts to overwrite from the first log file.

Properties Files

RiskFort primarily uses the properties files discussed in the following sub-sections:

- riskfort.risk-evaluation.properties
- riskfort.issuance.properties
- log4j.properties.risk-evaluation
- log4j.properties.riskfort-issuance

These files are available at:

`<install_location>\Arcot Systems\sdk\java\properties\`

riskfort.risk-evaluation.properties

The `riskfort.risk-evaluation.properties` file provides the parameters for the RiskFort Risk Evaluation Java SDK and Sample Application to read RiskFort Server information. Table B-13 lists the configuration parameters used in this file.

Table B-13. Parameters for Communication Between Risk Evaluation Java SDK and RiskFort Server

Parameter	Default	Description
HOST.1	localhost	IP address of RiskFort Server.
PORT.1	7680	Port number where RiskFort Server is listening to incoming requests.
CONNECTION_TIMEOUT	30000	Time in **milliseconds** before RiskFort Server is considered unreachable.
CONNECTION_RETRIES	1	Maximum number of retries allowed with RiskFort Server.
READ_TIMEOUT	30000	Maximum time in **milliseconds** allowed for a response from RiskFort Server.
MAX_ACTIVE	128	Maximum number of active connections (from the pool) allowed with RiskFort Server. It controls the maximum number of connections that can be borrowed from the pool at one time. When non-positive, there is no limit on the number of objects that might be active at a time.

Table B-13. Parameters for Communication Between Risk Evaluation Java SDK and RiskFort Server

Parameter	Default	Description
TIME_BETWEEN_CONNECTION_EVICTION	900000 (15 minutes)	Time in **milliseconds** between consecutive runs of the Idle Connection Evictor thread. **Important:** You must ensure that TIME_BETWEEN_CONNECTION_EVICTION + IDLE_TIME_OF_CONNECTION is less than the connection timeout of your firewall (between SDK and the RiskFort Server.) This will ensure no connection is abruptly dropped by the firewall because of idle time, which ensures smooth functioning of the system.
IDLE_TIME_OF_CONNECTION	1800000 (30 minutes)	Idle time (in **milliseconds**) after which a connection will be closed.
WHEN_EXHAUSTED_ACTION	BLOCK	The behavior when all connections are exhausted.

Table B-13. Parameters for Communication Between Risk Evaluation Java SDK and RiskFort Server

Parameter	Default	Description
TRANSPORT_TYPE	TCP	Default value for RiskFort Server to start up is TCP. Set this parameter to SSL, if RiskFort Native protocol is set to SSL. In other words, set this parameter to SSL, if you want to enable SSL-based secure communication between Administration Console and RiskFort Server. **Note:** You *must* restart RiskFort Server, if you change the value to SSL.
CA_CERT_FILE	*<server CA certificate (in PEM format) file path>*	Path for the CA certificate file of the server. The file *must* be in .PEM format. Provide the complete path for the file. For example: server.CACert=<*install_location*>/certs/ca.pem or server.CACert=<*install_location*>\\certs\\ca.pem **Note:** • Use CLIENT_P12_FILE for the client PKCS#12 file (which contains the Client key and the Certificate pair.) • Use CLIENT_P12_PASSWORD for the password of the specified PKCS#12 file.

riskfort.issuance.properties

The riskfort.issuance.properties file provides the parameters for the RiskFort Issuance Java SDK and Sample Application to read RiskFort Server information.

Note: Although this file has the same configuration parameters and default values as riskfort.risk-evaluation.properties, the values that you specify in this file can differ. You might need to do so to accommodate the time lag that occurs in Issuance-related operations.

Refer to Table B-13 for more information on configuration parameters in this file.

log4j.properties.risk-evaluation

The `log4j.properties.risk-evaluation` file specifies the logging behavior of RiskFort and its Risk Evaluation components. Table B-14 provides information on parameters that you need to configure for RiskFort Risk Evaluation.

Table B-14. Parameters for `log4j.properties.risk-evaluation` Configuration

Parameter	Default Value	Description
`log4j.logger.com.arcot`	INFO	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.
`log4j.logger.com.arcot.riskfortAPI`	DEBUG	
`log4j.appender.debuglog.File`	`arcot-riskfort-evaluaterisk.log`	The name of the log file. Possible values for this parameter are: • `riskfortsdk.log` (for RiskFort Java SDK) • `arriskfortws.log` (for RiskFort Web Service)
`log4j.appender.debuglog.MaxFileSize`	`1MB`	The maximum allowed file size of the log file.
`log4j.appender.debuglog.MaxBackupIndex`	`3`	The maximum number of backup files that can be created. When the number of backup files reaches this number, then the application starts to overwrite from the first log file.

log4j.properties.riskfort-issuance

The `log4j.properties.riskfort-issuance` file specifies the logging behavior of RiskFort and its Issuance components. Table B-15 provides information on parameters that you need to configure for RiskFort Issuance.

Table B-15. Parameters for `log4j.properties.riskfort-issuance` Configuration

Parameter	Default Value	Description
`log4j.logger.com.arcot`	INFO	Specify the log level that must be used to write the logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the log levels.
`log4j.logger.com.arcot.riskfortissuanceAPI`	DEBUG	
`log4j.appender.debuglog.File`	`arcot-riskfort-issuance.log`	The name of the log file. Possible values for this parameter are: • `arcotissuance.log` (for Issuance Java SDK) • `arissuancews.log` (for Issuance Web Service)
`log4j.appender.debuglog.MaxFileSize`	`1MB`	The maximum allowed file size of the log file.
`log4j.appender.debuglog.MaxBackupIndex`	`3`	The maximum number of backup files that can be created. When the number of backup files reaches this number, then the application starts to overwrite from the first log file.

Appendix C
Database Reference

RiskFort database contains a number of tables, some of which grow with increased usage of the product. Some tables grow in direct relation to the number of users, while others grow in direct relation to the usage of the product. Also, a user accessing the system multiple time will cause the tables to grow. Because of restricted disk space, as a database administrator managing RiskFort deployments, you might not want these tables to grow indefinitely. In this case, you can use the information in this appendix to trim some tables to manage your disk space and improve the database performance.

You must only trim the tables that capture transaction details, such as audit log information. You *must not* trim tables that capture user information, which is necessary to assess the risk evaluation.

Note: Arcot recommends that you make appropriate adjustments to the SQL databases based on the configuration and the need for reporting data. For example, deleting a large volume of data will adversely impact performance during the delete process. Depending on the size of the rollback segments, this may even cause the system to fail. It is also highly recommended that you archive older records and not delete them completely.

This appendix discusses the recommendations on database table replication, how to calculate the database size while you are planning to set up the database for RiskFort, and lists all tables used by RiskFort along with some trimming recommendations:

- RiskFort Database Tables
- Database Sizing Calculations
- Database Tables Replication Advice
- Database Tables Archival Recommendations
- Database Connection Tuning Parameters

RiskFort Database Tables

This section briefly explains all the database tables:

- Used by RiskFort
- Used by Administration Console and UDS

Used by RiskFort

Table C-1 lists all RiskFort database tables and their description.

Table C-1. RiskFort Tables

Table Name	Description
ARQGEOANONYMIZER1	Stores the known IP addresses of the anonymizers that do not propagate the end-user IP addresses. This is the primary table. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGeoAnonymizer2.
ARQGEOANONYMIZER2	Stores the known IP addresses of the anonymizers that do not propagate the end-user IP addresses. This is the secondary table. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGeoAnonymizer1.
ARQGEOPOINT1	Stores the geo-location information for different ranges of IP addresses. This information is obtained from Quova. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGEOPOINT2.
ARQGEOPOINT2	Stores the geo-location information for different ranges of IP addresses. This information is obtained from Quova. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGEOPOINT1.
ARQUOVAVERSION	Tracks the files from Quova that were uploaded to ARQ* tables.
ARREPORTTABLES	Contains the metadata of other tables.

Table C-1. RiskFort Tables

Table Name	Description
ARRF_CASE_TXN	Contains the Case-to-Transaction mapping and related details of the default Channel. If you define a specific Channel for your deployment, then another database table is created with the Channel name appended to the default table, for example, ARRF_CASE_TXN_<*channel_name*>.
ARRF_CMA	Contains the repeated transactions of the same combination of Cardholder-Merchant-Amount (CMA). **Note:** If the rule is not used, then the table is empty.
ARRF_IMA	Contains the repeated transactions of the same combination of IP-Merchant-Amount. **Note:** If the rule is not used, the table is empty.
ARRFADDONEXPOSEDPARAMS	Stores the parameter details used by the deployed Add-On rules. This table also stores the information whether specific parameters can be modified by an Add-On rule during processing. **Note:** It is recommended that you consult Arcot support at *support@arcot.com* before modifying any parameters.
ARRFADDONRULELISTDATA	Contains list data and corresponding dataset version. This is used by list lookup rules.
ARRFADDONRULEMAPPINGDATA	Contains mapping of the elements and the category to which it belongs to. This data is used by derived list lookup rules. For example, Merchant rules in a 3-D Secure deployment.
ARRFADDONRULETYPE	Stores the detailed configuration information for Add-On rules implemented for each organization in the system.
ARRFADVICECODE	Stores the list of available risk advices.
ARRFADVICECONFIG	Stores mapping of risk score ranges and corresponding advice. **Note:** Currently, this mapping is same for all the organizations.
ARRFCASEAUDITLOG	Stores the case details and other case-related activities that are logged.
ARRFCASECONFIG	Stores the configuration data for case management module.
ARRFCASEQUEUES	Stores the definitions of each case queue.

Table C-1. RiskFort Tables

Table Name	Description
ARRFCASES	Stores the details of all the open cases in the system, irrespective of the queue they belong to.
ARRFCHANNEL	Stores the basic definition (such as, case transaction table name and audit log table name) of all Channels that exist in the system.
ARRFCHANNELDETAILCATEGORY	Stores the details on various categories that GUI display elements belong to, for each channel.
ARRFCHANNELELEMENTS	Stores the details of all Channel elements.
ARRFCLIENTCERTSANDKEYS	Stores SSL keys and certificates required for communicating with a de-tokenization service. **Note:** Currently, this table is applicable only for TransFort-RiskFort integration deployments.
ARRFCLIENTSSLROOTCAS	Stores the client trust stores and the corresponding root CA certificates for two-way SSL authentication.
ARRFCONFIG	Stores global RiskFort configuration information.
ARRFCOUNTRY	Stores the list of all countries and their ISO codes.
ARRFCOUNTRYLIST	Stores the list of all countries as listed in Quova data.
ARRFCURRENCY	Stores the details of all currencies, their ISO codes, and exponents for each.
ARRFCURRENTORGCONFIG	Stores the current configuration for all organizations in the system.
ARRFDATAVERSIONMAPPING	Stores all configured RiskFort configuration information. The information in this table contains version information, and therefore can contain multiple entries per configuration.
ARRFDBERRORCODES	Contains all database error codes that indicate a possible communication failure. **Note:** It is recommended that you consult Arcot support at *support@arcot.com* before editing this table.
ARRFDEVICECONTEXT	Stores the context information (such as device status, timestamp of the transaction, and the requested action) for each incoming transaction from a user device. **Note:** This information is used for Device Velocity checks.

Table C-1. RiskFort Tables

Table Name	Description
ARRFDEVICEINFO	Stores the detailed information for all devices used for user transactions.
ARRFDEVICEINFOHIST	Stores history of all user devices registered with the system.
ARRFDEVUSERASSO	Stores all information related to user-device mapping.
ARRFDISPLAYNAMES	Stores all variable strings (for DISPLAYNAMEKEY) that are used by Administration Console labels (ARRFMESSAGES).
ARRFELEMENTSSUPPORTEDVALUES	Stores the Case Management layout details for viewing transaction details.
ARRFEXCEPTIONUSER	Stores the list of users marked as Exception Users.
ARRFEXCPUSERHIST	Stores the history of all users who were marked as exception users.
ARRFIPCONTEXT	Stores the IP context that is used by the IP velocity rule. **Note:** This table is for future use.
ARRFLIBRARYTOTYPEMAPPING	Stores the mapping of all supported Add-On rule types with the corresponding library name. **Note:** This table is for future use.
ARRFLOCALE	Stores information related to all supported locales.
ARRFMESSAGES	Stores the Response and Reason Codes messages.
ARRFNEGATIVECOUNTRYLIST	Stores the list of all negative countries.
ARRFORGCHANNEL	Stores the list of all supported Channels for each organization.
ARRFORGQUEUES	Stores the list and basic details of all queues belonging to an organization and Channel. **Note:** Currently, *only* one default queue is supported per organization.
ARRFPROTOCOLREGISTRY	Stores configuration of each listener port of the RiskFort Server.
ARRFQUEUEADMIN	Stores the Queue-to-Administrator mapping details.
ARRFSERVERS	Stores the mapping of available RiskFort Server instances.
ARRFSITES	Stores site details for each de-tokenization service. **Note:** Currently, this table is applicable only for TransFort-RiskFort integration deployments.

Table C-1. RiskFort Tables

Table Name	Description
ARRFSYSAUDITLOG	Stores all details related to risk evaluation and other activities that are logged. If you configure additional Channels for your deployment, then corresponding tables are created and named with the Channel name appended to the default table name, for example, ARRFSYSAUDITLOG_<*channel_name*>.
ARRFSYSORGCONFIG	Stores all versions of configurations available for all organizations in the system.
ARRFSYSPARAMSCONFIG	Contains detailed information about all RiskFort system parameters that are configurable by using the Administration Console.
ARRFSYSRULEEXECCONFIG	Stores the configuration information for all rules. This information includes version and configuration for each rule. **Note:** This table stores both history and the changes made by the administrator.
ARRFSYSTERMRULESCORECONFIG	Stores configuration information for each rule and the corresponding result that impacts the risk score.
ARRFTRUSTEDIPLIST	Stores the information for all trusted aggregators, IP addresses, and ranges.
ARRFUNTRUSTEDIPLIST	Stores the details of all negative IP addresses.
ARRFUNTRUSTEDIPTYPE	Stores the mapping for all supported negative IP types.
ARRFUPLOADAUDITLOG	Stores the details of the operations performed on the GeoPoint and GeoAnonymizer tables.
ARRFUSERCONTEXT	Stores the context information (such as user status, timestamp of the transaction, and the requested action) for each incoming transaction from a user. **Note:** This information is used for User Velocity checks.

Used by Administration Console and UDS

Table C-2 lists all RiskFort database tables and their description.

Table C-2. Administration Console Tables

Table Name	Description
Administration Console Tables	
ARADMINAUDITTRAIL	Contains administrator activity audit.
ARADMINBASICAUTHUSER	Contains the basic authentication credentials of the administrators.
ARADMINCACHEREFRESH	Contains cache refresh information that decides whether the Administration Console need to refresh the cache.
ARADMINCONFIG	Contains the Administration Console configurations.
ARADMINCUSTOMROLE	Contains the configurations for custom defined role.
ARADMINMANAGEROLE	Contains the list of roles that a role can manage.
ARADMINMAP	Contains the information of the RiskFort Server instance, which is entered as a key-value pair.
ARADMINMAPDATATYPE	Contains the list of data types that are supported in ARADMINMAP.
ARADMINPAFCONFIG	Contains administrator authentication configuration for an organization.
ARADMINPREDEFINEDROLE	Contains the role information for all supported administrators.
ARADMINPWDPOLICY	Contains the administrator password policies for all the organizations.
ARADMINROLEPRIVILEGE	Stores the mapping of all administrative actions (or tasks) supported by the Administration Console, the scope of each task, and which role can perform the task.
ARADMINSCOPE	Contains the information of the set of organizations over which an administrator has control.
ARADMINSCOPEALL	Contains the list of all administrators who have control over *all* the existing organizations in the system.
ARADMINSUPPORTEDAUTHMECH	Contains the information about all supported authentication mechanisms to log into the Administration Console.
ARADMINTURNEDOFFPRIVILEGE	Contains the information about the privileges that are not available for the given custom role.
ARADMINTXID	Contains the information required to generate a unique ID for each transaction.
ARADMINUITAB	Contains the information about the tabs that are available and the order in which they are available in the Administration Console.

Table C-2. Administration Console Tables

Table Name	Description
ARADMINUITASK	Contains the information about the tasks that are available and the order in which they are available through the Administration Console.
ARADMINUITASKATTRIBUTES	Contains the details of the tasks that are displayed, when the first-level and the second-level tabs in the Administration Console are clicked. These tasks are referred to as landing pages.
ARADMINUITASKCONTAINER	Contains the information related to available task containers. A task container can either be a second-level tab ID or the task group in the Administration Console.
ARADMINUSER	Contains the detailed information (such as organization to which they belong, current status, timezone, and locale) of all existing administrators.
ARADMINWIZARDTASK	Contains the information about all the tasks performed by using the Bootstrap Wizard.
ARCMNDBERRORCODES	Contains vendor-specific database error codes and SQL state values that signify whether the database is down or non-responsive. This information is used by the system to decide if database should be failed over, in case a backup database is configured.
UDS Tables	
ARUDSAUDITLOG	Contains the audit log information for the User Data Source (UDS) operations and their return status.
ARUDSAUTHSESSION	Contains authentication session details for currently active sessions. If this table is not replicated, then active authentication sessions can be lost.
ARUDSCONFIG	Contains the UDS configuration parameters and their values.
ARUDSORGANIZATION	Contains organization definitions, their attributes and repository connectivity details.
ARUDSREPOSITORYTYPES	Contains the definitions of all repositories supported by UDS.
ARUDSUSER	Contains user details and attributes of all users who belong to the organization.
ARUDSUSERATTRIBUTE	Contains all user attribute definitions. This table is expected to change rarely, only when new user attributes are added by individual products.

Database Sizing Calculations

This section helps database administrators to calculate the approximate size of the database that has to be set up for RiskFort.

Denotations Used in Sample Calculations

The following denotations are used in the sample calculation:

- Number of users = *N*
- Average number of devices per user = *O*
- Average number of user-device associations = *A*
- Average number of transactions per day = *T*
- Number of entries in the Quova Data Feed = *Q*
- Computation time frame (in days) = *D*

Value Assumptions Made

The following assumptions have been made for calculation purposes:

- Number of users (**N**) = 1,000,000 (one million)
- Average number of devices per user (**O**) = 2
- Average number of user-device associations (**A**) = 2
- Average number of transactions per day (**T**) = 24,000
- Number of entries in the Quova Data Feed (**Q**) = 10,000,000 (ten million)
- Computation time frames (**D**) = 90 days

Sample Calculations Based on Assumptions Made

Considering the figures assumed in the previous section the final requirement should be:

- Based on **total number of users**, the database size = `(10 * N)` KB

  In this calculation, the value `10 KB` per user has been arrived at as follows:

  - **ARRFUSERCONTEXT:** 3 KB per record
  - **ARUDSUSER:** 3.5 KB per record

- **ARUDSAUDITLOG:** 3 KB per record

- Based on **total number of devices**, the database size = `(6 * O * N)` KB

  In this calculation, the value `6 KB` per user has been arrived at as follows:

  - **ARRFDEVICECONTEXT:** 2 KB per record
  - **ARRFDEVICEINFO:** 4 KB per record

  In this calculation, based on the assumption made in the previous section:

  - **O**: 2

- Based on **total number of user-device associations**, the database size = `(5 * A * N)` KB

  In this calculation, the value `5 KB` per user has been arrived at as follows:

  - **DEVICEUSERASSOCIATION:** 1 KB per record
  - **DEVICEINFO:** 4 KB per record

  In this calculation, based on the assumption made in the previous section:

  - **A**: 2

- Based on **daily activity,** the database size = `(T * D * 20)` KB
- Based on the **size of Quova Data Feed,** the database size = `(Q * 2)` KB

Database Tables Replication Advice

This section provides information on how frequently the tables must be replicated between the primary and the backup databases. It covers the following topics:

- Tables That Need Real-Time Synchronization
- Tables That Need Periodic Synchronization
- Tables That Do Not Need Synchronization

Tables That Need Real-Time Synchronization

Table C-3 lists the database tables that need real-time synchronization between the primary and the backup databases. This category mainly includes the tables that contain user-related information and this data is required for authentication, therefore you must perform real-time synchronization of these tables.

Table C-3. Tables That Need Real-Time Synchronization

Table	Description
ARADMINAUDITTRAIL	Contains the audit log information for the RiskFort administration activities.
ARADMINBASICAUTHUSER	Contains the basic authentication credentials of the administrators.
ARADMINSCOPE	Contains the information of the set of organizations over which an administrator has control.
ARADMINSCOPEALL	Contains the list of administrator who have control over all the organizations that are existing and those that will be created in future.
ARADMINUSER	Contains the information of an administrator.
ARADMINTXID	Contains the information required to generate transaction ID.
ARUDSORGANIZATION	Contains organization definitions, their attributes and repository connectivity details.
ARUDSUSER	Contains user details and attributes of the users belonging to the organization. Also contains PAM, if any, for all types of users.
ARUDSAUTHSESSION	Contains authentication session details for currently active sessions. If this table is not replicated, then active authentication session can be lost.
ARRF_CMA	Contains the repeated transactions of the same combination of Cardholder-Merchant-Amount (CMA). **Note:** If the rule is not used, then the table is empty.
ARRF_IMA	Contains the repeated transactions of the same combination of IP-Merchant-Amount. **Note:** If the rule is not used, the table is empty.
ARRF_CASE_TXN	Contains the Case-to-Transaction mapping and related details of the default Channel. If you define a specific Channel for your deployment, then another database table is created with the Channel name appended to the default table, for example, ARRF_CASE_TXN_*<channel_name>*.
ARRFADDONRULELISTDATA	Contains list data and corresponding dataset version. This is used by list lookup rules.

Table C-3. Tables That Need Real-Time Synchronization

Table	Description
ARRFADDONRULEMAPPINGDATA	Contains mapping of the elements and the category to which it belongs to. This data is used by derived list lookup rules. For example, Merchant rules in a 3-D Secure deployment.
ARRFCASEAUDITLOG	Stores the case details and other case-related activities that are logged.
ARRFCLIENTSSLROOTCAS	Stores the client trust stores and the corresponding root CA certificates for two-way SSL authentication.
ARRFCURRENTORGCONFIG	Stores the current configuration for all organizations in the system.
ARRFDATAVERSIONMAPPING	Stores all configured RiskFort configuration information. The information in this table contains version information, and therefore can contain multiple entries per configuration.
ARRFDEVICECONTEXT	Stores the context information (such as device status, timestamp of the transaction, and the requested action) for each incoming transaction from a user device. **Note:** This information is used for Device Velocity checks.
ARRFDEVICEINFO	Stores the detailed information for all devices used for user transactions.
ARRFDEVUSERASSO	Stores all information related to user-device mapping.
ARRFEXCEPTIONUSER	Stores the list of users marked as Exception Users.
ARRFIPCONTEXT	Stores the IP context that is used by the IP velocity rule. **Note:** This table is for future use.
ARRFNEGATIVECOUNTRYLIST	Stores the list of all negative countries.
ARRFSYSPARAMSCONFIG	Contains detailed information about all RiskFort system parameters that are configurable by using the Administration Console.
ARUDSAUDITLOG	Contains the audit log information for the User Data Source (UDS) operations and their return status.
ARRFSYSAUDITLOG	Stores all details related to risk evaluation and other activities that are logged. If you configure additional Channels for your deployment, then corresponding tables are created and named with the Channel name appended to the default table name, for example, ARRFSYSAUDITLOG_<*channel_name*>.

Table C-3. Tables That Need Real-Time Synchronization

Table	Description
ARRFSYSORGCONFIG	Stores all versions of configurations available for all organizations in the system.
ARRFSYSRULEEXECCONFIG	Stores the configuration information for all rules. This information includes version and configuration for each rule. **Note:** This table stores both history and the changes made by the administrator.
ARRFSYSTERMRULESCORECONFIG	Stores configuration information for each rule and the corresponding result that impacts the risk score.
ARRFTRUSTEDIPLIST	Stores the information for all trusted aggregators, IP addresses, and ranges.
ARRFUNTRUSTEDIPLIST	Stores the details of all negative IP addresses.
ARRFUSERCONTEXT	Stores the context information (such as user status, timestamp of the transaction, and the requested action) for each incoming transaction from a user. **Note:** This information is used for User Velocity checks.
ARSEQUENCETABLE	Contains the information to track sequence values required by MS SQL.

Tables That Need Periodic Synchronization

Table C-4 lists the database tables that need periodic synchronization between the primary and the backup databases. These database tables are synchronized when there is any change in the configurations.

Table C-4. Periodic Synchronization Tables

Table	Description
ARADMINCONFIG	Contains the Administration Console configurations.
ARADMINCUSTOMROLE	Contains the configurations for custom defined role.
ARADMINMAP	Contains the information of the RiskFort Server instance, which is entered as a key-value pair.
ARADMINPAFCONFIG	Contains administrator authentication configuration for an organization.

Table C-4. Periodic Synchronization Tables

ARADMINPWDPOLICY	Contains the administrator password policies for all the organizations.
ARADMINTURNEDOFFPRIVILEGE	Contains the information about the privileges that are not available for the custom role.
ARADMINCACHEREFRESH	Contains cache refresh information that decides whether the Administration Console need to refresh the cache.
ARRFCHANNEL	Stores the basic definition (such as, case transaction table name and audit log table name) of all Channels that exist in the system.
ARRFCHANNELDETAILCATEGORY	Stores the details on various categories that GUI display elements belong to, for each channel.
ARRFCHANNELELEMENTS	Stores the details of all Channel elements.
ARUDSCONFIG	Contains the UDS configuration parameters and their values.
ARUDSREPOSITORYTYPES	Contains the definitions of the repository supported by UDS. This table is expected to change only when new plug-ins are added to the system.
ARUDSUSERATTRIBUTE	Contains the user attribute definitions. This table is expected to change rarely, only when new user attributes are added by individual products.
ARQGEOANONYMIZER1	Stores the known IP addresses of the anonymizers that do not propagate the end-user IP addresses. This is the primary table. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGeoAnonymizer2.
ARQGEOANONYMIZER2	Stores the known IP addresses of the anonymizers that do not propagate the end-user IP addresses. This is the secondary table. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGeoAnonymizer1.
ARQGEOPOINT1	Stores the geo-location information for different ranges of IP addresses. This information is obtained from Quova. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGeoPoint2.

Table C-4. Periodic Synchronization Tables

ARQGEOPOINT2	Stores the geo-location information for different ranges of IP addresses. This information is obtained from Quova. **Note:** While reloading data to this table, RiskFort Server will refer to ARQGeoPoint1.
ARQUOVAVERSION	Tracks the files from Quova that were uploaded to ARQ* tables.
ARRFADDONRULETYPE	Stores the detailed configuration information for Add-On rules implemented for each organization in the system.
ARRFADVICECONFIG	Stores mapping of risk score ranges and corresponding advice. **Note:** Currently, this mapping is same for all the organizations.
ARRFCASEQUEUES	Stores the definitions of each case queue.
ARRFCONFIG	Stores global RiskFort configuration information.
ARRFCLIENTCERTSANDKEYS	Stores SSL keys and certificates required for communicating with de-tokenization service. **Note:** Currently, this table is applicable only for TransFort-RiskFort integration deployments.
ARRFDEVICEINFOHIST	Stores history of all user devices registered with the system.
ARRFELEMENTSSUPPORTEDVALUES	Stores the Case Management layout details for viewing transaction details.
ARRFEXCPUSERHIST	Stores the history of all users who were marked as exception users.
ARRFLIBRARYTOTYPEMAPPING	Stores the mapping of all supported Add-On rule types with the corresponding library name. This table is for future use.
ARRFORGCHANNEL	Stores the list of all supported Channels for each organization.
ARRFORGQUEUES	Stores the list and basic details of all queues belonging to an organization and Channel. **Note:** Currently, *only* one default queue is supported per organization.
ARRFPROTOCOLREGISTRY	Stores configuration of each listener port of the RiskFort Server.

Table C-4. Periodic Synchronization Tables

ARRFQUEUEADMIN	Stores the Queue-to-Administrator mapping details.
ARRFSERVERS	Stores the mapping of available RiskFort Server instances.
ARRFSITES	Stores site details for each de-tokenization service. **Note:** Currently, this table is applicable only for TransFort-RiskFort integration deployments.
ARRFUNTRUSTEDIPTYPE	Stores the mapping for all supported negative IP types.
ARRFUPLOADAUDITLOG	Stores the details of the operations performed on the GeoPoint and GeoAnonymizer tables.

Tables That Do Not Need Synchronization

Table C-5 lists the database tables that do not need any synchronization between the primary and the backup databases.

Table C-5. Tables That Do Not Need Synchronization

Table	Description
ARCMNDBERRORCODES	Contains vendor-specific database error codes and SQL state values that signifies whether the database is down or non-responsive. This information is used to decide if database should be failed over, if a backup is configured.
ARADMINMANAGEROLE	Contains the list of roles that a role can manage.
ARADMINPREDEFINEDROLE	Contains the role information for all supported administrators.
ARADMINSUPPORTEDAUTHMECH	Contains the information about all supported authentication mechanisms.
ARADMINUITAB	Contains the information about Administration Console tabs.
ARADMINUITASK	Contains the information about the tasks that are performed using Administration Console.
ARADMINUITASKATTRIBUTES	Contains the details of the tasks that are displayed, when the first-level and the second-level tabs in the Administration Console are clicked. These tasks are referred to as landing pages.
ARADMINUITASKCONTAINER	Contains the information related to the task container. The task container can either be a second-level tab ID or the task group in the Administration Console.

Table C-5. Tables That Do Not Need Synchronization

Table	Description
ARADMINWIZARDTASK	Contains the information about the tasks that are performed using the Administration Console bootstrap wizard.
ARREPORTTABLES	Contains the metadata of other tables.
ARADMINMAPDATATYPE	Contains the list of data types that are supported in ARADMINMAP.
ARRFADVICECODE	Stores the list of available risk advices.
ARRFADDONEXPOSEDPARAMS	Stores the parameter details used by the deployed Add-On rules. This table also stores the information whether specific parameters can be modified by an Add-On rule during processing. **Note:** It is recommended that you consult Arcot support at *support@arcot.com* before modifying any parameters.
ARRFCASECONFIG	Stores the configuration data for case management module.
ARRFCOUNTRY	Stores the list of all countries and their ISO codes.
ARRFCOUNTRYLIST	Stores the list of all countries as listed in Quova data.
ARRFCURRENCY	Stores the details of all currencies, their ISO codes, and exponents for each.
ARRFDBERRORCODES	Contains all database error codes that indicate a possible communication failure. **Note:** It is recommended that you consult Arcot support at *support@arcot.com* before editing this table.
ARRFDISPLAYNAMES	Stores all variable strings (for DISPLAYNAMEKEY) that are used by Administration Console labels (ARRFMESSAGES).
ARRFLOCALE	Stores information related to all supported locales.
ARRFMESSAGES	Stores the Response and Reason Codes messages.

Database Tables Archival Recommendations

The tables discussed in this section grow continuously with every transaction, but are not required for risk scoring. As a result, these can be trimmed. These tables are:

- **ARRFSYSAUDITLOG**

This table stores the audit log information. There is an entry in this table for every transaction by RiskFort. By deleting entries from this table, the amount of available reporting data is reduced.

- **ARADMINAUDITTRIAL**

  This table contains the history of all actions performed by administrators.

ARUDSUSER

It is highly recommended that you only trim the tables that capture transaction details, such as audit log information. You *must not* trim tables that capture user information, which is necessary to assess the risk evaluation.

However, in some cases, you can choose to archive user data in the ARUDSUSER table. For example, you might want to archive information for users who have not accessed the application for a specified duration. In such cases, you can treat the returning user as a new user and provide risk scores consistent with that classification.

Note: If your organization is interested in such optimizations, then it is recommended that you work with Arcot's Professional Services team for the same.

An entry in the ARUDSUSER table for a user represents an enrolled user. The basic information of the user is stored in this table. User record enters in to this table through RiskFort Issuance API.

Database Connection Tuning Parameters

The parameters that you can use to tune the connection between RiskFort Server and the database are configured in the arcotcommon.ini file.

Appendix D
Default Port Numbers and URLs

This appendix lists the default port numbers and URLs that RiskFort uses. It contains the following sections:

- Default Port Numbers
- URLs for RiskFort Components

Default Port Numbers

During the installation, the installer checks if the required default port number is in use. If the port number is not in use, then the installer assigns it to the RiskFort component. However, if the default port number is already in use by an Arcot product or by any other application, then you must specify the port number manually by using the RiskFort Protocol Setup screen in the Administration Console.

Table D-1 lists the default port numbers used by RiskFort.

Table D-1. RiskFort Protocols and Port Numbers

Protocol	Default Port Number	Description
RiskFort Native (TCP)	7680	This is an Arcot proprietary protocol to enable communication between the RiskFort Server instance and the RiskFort Java SDKs (which include Risk Evaluation and Issuance.)
Native (SSL)	7681	This is an Arcot proprietary protocol to enable SSL-based communication between the RiskFort Server instance and the RiskFort Java SDKs (which include Risk Evaluation and Issuance.)

Table D-1. RiskFort Protocols and Port Numbers

Protocol	Default Port Number	Description
Administration Web Service	7777	This is the protocol for communication between RiskFort Server and Administration Web services. The RiskFort Server listens to the Administration Web service calls on this port. **Note:** These calls do *not* include the RiskFort Issuance or Risk Evaluation calls.
Transaction Web Service	7778	This protocol is used by the Risk Evaluation and the Issuance Web services to connect to the RiskFort Server instance. **Note:** These calls do *not* include the Administration service calls.
Queueing 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.
Queueing Administration	7780	This is the protocol for communication between RiskFort Server and Queuing Management. The RiskFort Server listens to the Case Management Web service calls on this port.
Server Management	7980	The `arrfadmin` tool communicates with the RiskFort Server instance for server management activities (graceful shutdown and server cache refresh) by using this protocol. **Book:** See *Arcot RiskFort 2.2.6 Administration Guide* for detailed information on this Administration Console tool.

URLs for RiskFort Components

Use the URLs listed in the Table D-2 to access RiskFort components after installation. The URLs in the table use the default ports.

Table D-2. Default Port Numbers

Component or Service	URL
Administration Console (For Master Administrator (MA))	*http://<hostname>:<port>/arcotadmin/masteradminlogin.htm* **Note:** The port that you must specify here is your application server port.
Administration Console (For Other Administrators)	*http://<hostname>:<port>/arcotadmin/adminlogin.htm* **Note:** The port that you must specify here is your application server port.
Sample Application	*http://<hostname>:<port>/riskfort-2.2.6-sample-application/index.jsp* **Note:** The port that you must specify here is your application server port.
Issuance Web Service	*http://<hostname>:<port>/services/RiskFortIssuanceSvc* **Note:** The default port here is 7778.
Risk Evaluation Web Service	*http://<hostname>:<port>/services/RiskFortEvaluateRiskSvc* **Note:** The default port here is 7778.

Appendix E
Configuring Application Server for Database Connection Pooling

This appendix quickly walks you through the steps to set up database connection pooling on the application server, where you will deploy RiskFort components. The configuration steps for the following application servers are covered:

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Apache Tomcat

This section provides the steps to enable Apache Tomcat for JNDI-based database operations. To create a JNDI connection in Apache Tomcat:

1. Install the Apache Tomcat application server and test the installation using the following URL:

   http://localhost:8080/

2. Open the `server.xml` file present in the `<TOMCAT_HOME>/conf/` directory.
3. Collect the following information required to define a data source:
   - **JNDI Name**

     The JNDI name used by the arcot components.

	**Important:** This name *must* match with the `AppServerConnectionPoolName.<N>` in arcotcommon.ini (*without* the `java:comp/env/` prefix).

   - **User ID**

     The database user ID.
   - **Password**

The database password.

- **JDBC Driver Class**

  The JDBC driver class name, for example:

  `oracle.jdbc.driver.OracleDriver`

- **JDBC URL**

  The JDBC URL for the database server, for example if you are using the Oracle driver, then URL will be:

  `jdbc:oracle:thin:<server>:<port>:<sid>`

4. Add the following entry to define the data source within the `<GlobalNamingResources>` tag:

```
<Resource name="SampleDS"
        auth="Container"
        type="javax.sql.DataSource"
factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory"
        username="<userid>"
        password="<password>"
        driverClassName="<JDBC driver class>"
        url="<jdbc-url>"
        maxWait="30000"
        maxActive="32"
        maxIdle="8"
        initialSize="4"
        timeBetweenEvictionRunsMillis="300000"
        minEvictableIdleTimeMillis="30000"/>
```

5. Open the `context.xml` file available in the `<TOMCAT_HOME>/conf/` directory.
6. Add the following entry to define the datasource within the `<Context>` tag:

```
<ResourceLink global="SampleDS" name="SampleDS"
type="javax.sql.DataSource"/>
```

7. Copy the following database connection pooling (DBCP) dependencies to the `<TOMCAT_HOME>/common/lib/` directory:
   - `commons-dbcp-1.2.2.jar`
   - `ojdbc14-10.2.0.1.0.jar` (for Oracle database)
   - `sqljdbc.jar` (Microsoft JDBC driver for MS SQL Server 2005 - version 1.2.2828)

IBM WebSphere

This section provides the steps to enable IBM WebSphere for JNDI-based database operations. To configure an IBM WebSphere instance for deploying Java-dependant components of RiskFort:

1. Log in to WebSphere Administration Console.
2. Select **Resources** and expand the **JDBC** node.
3. Select **JDBC Providers** and click **New** to create an appropriate JDBC provider based on the database that you are using.

Note: For more information, refer to: *http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.iseries.doc/info/iseries/ae/tdat_ccrtprov.html*

4. Enter the database `CLASSPATH` information by following the on-screen instructions.
5. Click **Next** and verify the Summary page. Click **Finish** to complete the JDBC provider configuration.
6. Click **Save** to save the changes.
7. Navigate to **Resources**, and then click **JDBC**.
8. Under **JDBC**, open **Data Sources** and click **New** to create a new data source:
   a. Specify the **Data Source Name**.
   b. Specify the **JNDI Name**.

Note: This name *must* match with the value of `AppServerConnectionPoolName.<N>` in `arcotcommon.ini`.

c. Click **Next** and select the **JDBC Provider** that you created in Step 3.

d. Click **Next** and specify the **JDBC URL**.

e. Select the data source and click **Next** and then **Finish**.

f. Click **Next** to view the Summary page and then click **Finish**.

9. Click **Save** to save the changes.
10. Select the data source that you created in the preceding steps and click the **Related Items** section.
11. Select **New** to create a new credential.
12. Enter login credentials that are used to connect to the database and save the credential.
13. Click **Apply** and then **Save** to save the changes.
14. Select **Data Sources** and select the data source that you created in Step 7.
15. Under **Component-managed authentication alias**, select the JAAS credential that you created in Step 12 and click **Save**.
16. Select **Data Sources** and select the check box for the data source you created in Step 7.
17. Click **Test Connection** to verify that you have specified the connection correctly.

Note: This test only checks the connection to the database server. It does *not* verify the correct definition of the data source.

BEA WebLogic

This section walks you through the steps to enable BEA WebLogic for JNDI-based database operations. To create a data source for RiskFort in BEA WebLogic:

1. Log in to WebLogic Administration Console.
2. Click the **Lock & Edit** button in the Change Center, if it is not already done.
3. Navigate to **Services**, **JDBC**, and the **Data Sources**.
4. Under **JDBC**, open **Data Sources** and click **New** to open the Create a New JDBC Data Source page.
5. Set the following JNDI and the database information:

a. Set **Name** = `ArcotDB`

b. Set **JNDI Name** = `ArcotDB`

c. Select the required **Database Type**, for example Oracle.

d. Select the required **Database Driver**, for example Oracle Thin Driver.

6. Click **Next**, retain the default values and click **Next** again.
7. In the Connection Properties page that appears, set the database connection details. For example, the values are for **Oracle** can be:
   - **Database Name** = SID or service name of the database server
   - **Host Name** = Host name or the IP address of the database server
   - **Port** = 1521 or any other port the database server is running
   - **Database User Name** = Database account user name that can create the database connections
   - **Password** / **Confirm Password** = Password for the specified Database User Name
8. Click **Test Configuration** to verify the database information that you specified.
9. Click **Next** and set the preferred data source target server for the WebLogic server instance.
10. Click **Finish** to return to the data source list page.
11. Click the **Activate** button in the Change Center to enable the data source settings that you configured in the preceding steps.

Appendix F
Configuring SSL

By default, RiskFort components use Transmission Control Protocol (TCP) to communicate with each other. However, TCP is vulnerable to spoofing and man-in-the-middle attacks. To ensure secure communication between Administration Console and RiskFort Server and between SDKs and RiskFort Server, you can configure RiskFort Native and Server Management protocols to support SSL (Secure Socket Layer), which ensures securer communication between applications across insecure media and reduces the chances of TCP attacks.

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

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

1. Enable UDS for SSL
2. Enable SSL Between Administration Console and User Data Service
3. Enable SSL Between RiskFort Server and User Data Service
4. Enable SSL Between Administration Console and RiskFort Server
5. Enable SSL Between Java SDKs and RiskFort Server
6. Enable SSL Between arrfadmin Tool and RiskFort Server

Enable UDS for SSL

The application server where User Data Service (UDS) is deployed must be enabled for SSL.

Note: Refer to your application server vendor documentation for more information.

Enable SSL Between Administration Console and User Data Service

If Administration Console and UDS are deployed on different application servers, then the application servers must be enabled for SSL.

Note: Refer to your application server vendor documentation for more information on how to set SSL.

Enable SSL Between RiskFort Server and User Data Service

To set up SSL between RiskFort Server and User Data Service (UDS), you must upload the certificates required for SSL by using the **User Data Service Configuration** page either while bootstrapping the system or later by using the Administration Console.

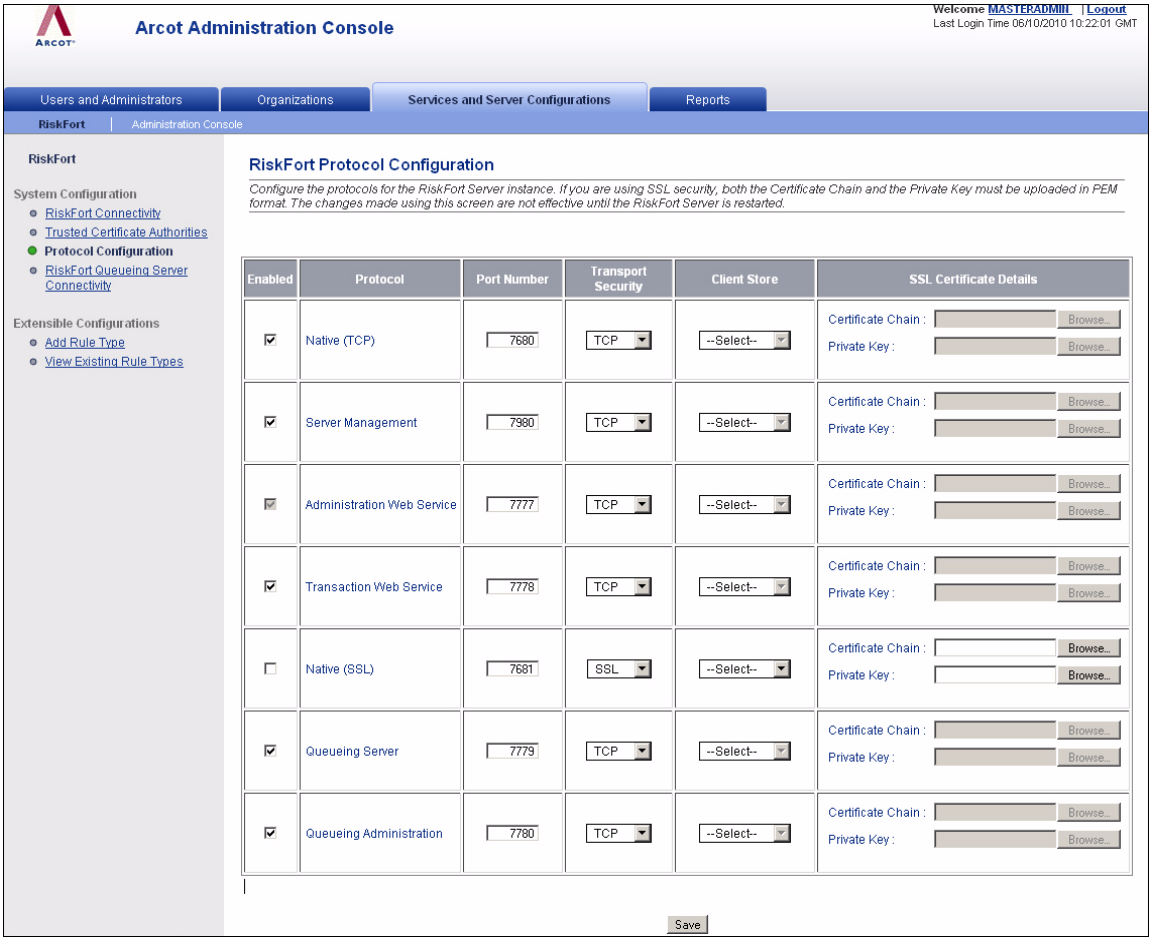
See, "Bootstrapping the System" for more information.

Enable SSL Between Administration Console and RiskFort Server

To configure SSL-based communication between RiskFort Server and Administration Console:

1. Open Administration Console in a Web browser.
2. Log in to Administration Console using the Master Administrator (MA) credentials.
3. Activate the **Services and Server Configurations** tab.
4. Ensure that the **RiskFort** option on the tab's sub-menu is selected.
5. Under the **System Configurations** section, click the **Protocol Configuration** link to display the RiskFort Protocol Configuration page (Figure F-1.)

Figure F-1 RiskFort Protocol Configuration Page



6. Configure the **Administration Web Service** protocol as follows:

   a. In the **Enabled** column, ensure that the box corresponding to **Administration Web Service** is selected.

   b. In the **Port Number** column, specify the required port number in the corresponding field.

   c. In the **Transport Security** column, select **SSL** from the drop-down list.

   d. In the **Client Store** column, select the required trust store that contains the root certificate of the trusted Certificate Authority (CA) from the drop-down list.

e. In the **SSL Certificate Details** column:

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

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

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

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

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

7. If not already displayed, click **RiskFort Connectivity** in the tasks pane to display the corresponding page.
8. Use the information in Table F-1 to edit the fields on the RiskFort Connectivity page.

Table F-1. RiskFort Connection Parameters

Field	Description
Server	Enter the IP address of the system where you installed the required RiskFort Server instance. **NOTE:** Ensure that the system where RiskFort Server is installed must be accessible by its `hostname` on the network.
Port	Enter the port on which the Administration Web Service is exposed.
Transport	Specify the transport mode as **SSL** for the Administration Console to connect to the specified RiskFort Server instance.
Server CA Root Certificate	Browse to and upload the PKCS#12 Store path that contains the server 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 path that contains the client certificate and the private key. **NOTE:** This client certificate must be in PEM format.
Client PKCS#12 Password	Enter the password for the client's PKCS#12 Store.

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

Note: If you add a new RiskFort Server instance, then before proceeding with the instance-specific configurations you must click **Save** in this page. This ensures that the Administration Console gets the details of all instances and the instance management functions will work smoothly for all instances.

10. Restart the RiskFort Server.
11. Restart the Administration Console.

Enable SSL Between Java SDKs and RiskFort Server

To enable SSL communication between RiskFort Server and Java SDKs, you must first configure the RiskFort Native protocol by using the Administration Console and then configure the applicable properties files:

- `<install_location>\Arcot Systems\sdk\java\properties\` **`riskfort.risk-evaluation.properties`**
- `<install_location>\Arcot Systems\sdk\java\properties\` **`riskfort.issuance.properties`**

To enable SSL communication mode between RiskFort Server and Java SDKs:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **System Configurations** section, click the **Protocol Configuration** link to display the Protocol Configuration page (Figure F-1.)
5. Configure the **Native (SSL)** protocol as follows:
    a. In the **Enabled** column, ensure that the box corresponding to **RiskFort Native** is selected.
    b. In the **Port Number** column, specify the required port number in the corresponding field.
    c. In the **Transport Security** column, select **SSL** from the drop-down list.
    d. In the **Client Store** column, select the required trust store that contains the root certificate of the trusted Certificate Authority (CA) from the drop-down list.
    e. In the **SSL Certificate Details** column:

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

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

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

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

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

6. Navigate to the following location on the system where the RiskFort Java SDK is deployed:

   `<install_location>\Arcot Systems\sdk\java\properties\`

7. Open the `riskfort.risk-evaluation.properties` file in an editor window.

   a. Set the following parameters:

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

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

      See riskfort.risk-evaluation.properties" for more information on the configuration parameters.

   b. Save the changes and close the file.

8. Open the `riskfort.issuance.properties` file in an editor window.

   a. Set the following parameters:

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

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

See riskfort.issuance.properties for more information on the configuration parameters.

b. Save the changes and close the file.

9. Restart RiskFort Server.
10. Restart the application server where the RiskFort Java SDK is deployed.

Enable SSL Between arrfadmin Tool and RiskFort Server

To enable SSL communication between the `arrfadmin` tool and the Administration Console, you must first configure the Server Management protocol by using the Administration Console and then configure the applicable INI file:

- `<install_location>\Arcot Systems\sdk\java\properties\` **`riskfortadminclient.ini`**

Note: See *Arcot RiskFort 2.2.6 Administration Guide* for more information on the `arrfadmin` tool.

To enable SSL communication mode between RiskFort Server and Java SDKs:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **RiskFort** tab in the sub menu is active.
4. Under the **System Configurations** section, click the **Protocol Configuration** link to display the Protocol Configuration page (Figure F-1.)
5. Configure the **Server Management** protocol as follows:
   a. In the **Enabled** column, ensure that the box corresponding to **Server Management** is selected.
   b. In the **Port Number** column, specify the required port number in the corresponding field.
   c. In the **Transport Security** column, select **SSL** from the drop-down list.
   d. In the **Client Store** column, select the required trust store that contains the root certificate of the trusted Certificate Authority (CA) from the drop-down list.
   e. In the **SSL Certificate Details** column:

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

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

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

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

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

6. Navigate to the following location:

   `<install_location>\Arcot Systems\conf\`

7. (**If you need two-way SSL communication**) Open the `riskfortadminclient.ini` file in an editor window.

   a. Set the following parameters:

   - `Host` (By default, this parameter is set to `localhost`.)
   - `Port` (By default, this parameter is set to `7980`.)
   - `Transport=SSL` (By default, this parameter is set to `TCP`.)
   - `SSLClientKey=<absolute_path_of_Client_SSL_Key_in_PEM_FORMAT>`
   - `SSLClientCertChain=<absolute_path_of_Client_SSL_Certificate_or Chain_in_PEM_FORMAT>`
   - `SSLServerCACert=<absolute_path_of_Server_Root_SSL_Certificate_in_ PEM_FORMAT>`

   For example, you can specify

   `SSLServerCACert=<install_location>/certs/<ca_cert>.pem`.

   See riskfortadminclient.ini for more information on the configuration parameters.

   b. Save the changes and close the file.

8. Restart RiskFort Server.
9. Restart the application server.

Appendix G
Third-Party Software Licenses

This appendix lists the third-party software packages that are used by RiskFort. These include:

Aspect-Oriented Programming (AOP) Alliance

- `aopalliance-1.0.jar`

Licensed under Public Domain (for AOP Alliance.) (*http://aopalliance.sourceforge.net/*)

ANTLR 2

- `antlr-2.7.6.jar`
- `antlr-2.7.7.jar`

Copyright © 2003-2006, Terence Parr. (*http://www.antlr.org/license.html*)

Licensed under Public Domain. (*https://olex.openlogic.com/licenses/4*)

Apache

Copyright © The Apache Software Foundation. Licensed under the **Apache License, Version 1.1**. (*http://www.apache.org/licenses/LICENSE-1.1.html*)

- `jakarta-oro-2.0.7.jar`

Copyright © The Apache Software Foundation. Licensed under the **Apache License, Version 2.0**. (*http://www.apache.org/licenses/*)

- `ant-1.7.0.jar`
- `axiom-impl-1.2.7.jar`
- `Axis2-1.4.jar`
- `cglib-2.1_3.jar`
- `commons-beanutils-1.7.0.jar`
- `commons-codec-1.3.jar`
- `commons-collections-3.1.jar`
- `commons-dbcp-1.2.2.jar`
- `commons-digester-1.7.jar`
- `commons-fileupload-1.1.1.jar`

- commons-fileupload-1.2.jar
- commons-httpclient-3.1.jar
- commons-io-1.2.jar
- commons-io-1.4.jar
- commons-lang-2.4.jar
- commons-logging-1.1.jar
- commons-logging-1.1.1.jar
- commons-pool-1.3.jar
- commons-pool-1.4.jar
- commons-validator-1.3.1.jar
- geronimo-activation-1.1.jar
- geronimo-annotation-1.0.jar
- geronimo-javamail-1.4.jar
- geronimo-jms.1.1.jar
- geronimo-stax-api-1.0.jar
- httpcore-4.0.jar
- iBATIS-2.3.4.726.jar
- jdom-1.0.jar
- jdom-1.1.jar
- jettison-1.0.1.jar
- jstl-api-1.1.2.jar
- jstl-standard-1.1.2.jar
- log4j.1.2.9.jar
- neethi-2.0.jar
- neethi-2.0.4.jar
- standard-1.1.2.jar
- stax-api-1.0.1.jar
- struts-1.2.8.jar
- velocity-1.5.jar
- woden-1.0.0.jar
- xbean-2.2.0.jar

- xbean-2.3.0.jar
- xercesImpl-2.8.1.jar
- xml.resolver-1.2.0.jar
- xml-commons-1.3.04.jar
- xml-xalan-2.7.0.jar
- xmlParserAPIs-2.6.0.jar
- XmlSchema-1.2.jar
- XmlSchema-1.4.2.jar

ASM

- asm-1.5.3.jar

Copyright © 2000-2005 INRIA, France Telecom. All rights reserved.
(*http://asm.ow2.org/license.html*)

Backport-Util-Concurrent

- backport-util-concurrent-2.2.jar

Copyright © 2004-2007 Distributed Computing Laboratory, Emory University.
(*http://backport-jsr166.sourceforge.net/*)

Licensed under Creative Commons Public Domain License.
(*http://creativecommons.org/licenses/by/3.0/*)

Bouncy Castle

- bcprov-jdk14-139.jar
- bcprov-jdk14-131.jar

Copyright © 2000 - 2009 The Legion Of The Bouncy Castle
(*http://www.bouncycastle.org/license.html*).

Codehaus Annogen

- annogen-0.1.0.jar

Copyright © 2003-2006 - The Codehaus. All rights reserved unless otherwise noted.
(*http://annogen.codehaus.org//*)

Licensed under Apache License, Version 2.0. (*http://www.apache.org/licenses/*)

- Java XPath Engine

Copyright © 2003-2006 The Werken Company. All Rights Reserved. (*http://jaxen.org/license.html*)

- `jaxen-1.1.jar`
- `jaxen-1.1.1.jar`

Cryptix

Copyright © 1995-2005 The Cryptix Foundation Limited. All rights reserved. (*http://www.cryptix.org/LICENSE.TXT*)

DOM4j

- `dom4j-1.6.1.jar`

Copyright 2001-2005 © MetaStuff, Ltd. All Rights Reserved. (*http://www.dom4j.org/license.html*)

Licensed under Apache Software License 1.1 , BSD style license. (*http://dom4j.sourceforge.net/dom4j-1.6.1/license.html*)

gSOAP 2.7.10

Copyright © 2000-2006 Robert A. van Engelen, Genivia, Inc. All Rights Reserved.

gSOAP Public License version 1.3b. (*http://www.cs.fsu.edu/~engelen/license.html*)

Hibernate Core 3.1

Copyright © 2006, Red Hat Middleware, LLC. All rights reserved. JBoss and Hibernate are registered trademarks and servicemarks of Red Hat, Inc. (*https://www.hibernate.org/*)

ICU License - ICU 1.8.1 and later

- `icu4j-2.6.1.jar`

Copyright © 1995-2010 International Business Machines Corporation and others (*http://source.icu-project.org/repos/icu/icu/trunk/license.html*)

JavaScript Object Notation Lib (JSON-Lib)

- `json-lib-0.7.1.jar`

Copyright © 2002 JSON.org. (*http://www.json.org/license.html*)

Licensed under Apache Software License 2.0. (*http://www.apache.org/licenses/LICENSE-2.0.html*)

JiBX: Binding XML to Java Code

- `jibx-bind-1.1.5.jar`

Microsoft SQL Server 2005 JDBC Driver

Open Source Initiative (OSI)

Common Development And Distribution License (CDDL) Version 1.0. (*http://www.opensource.org/licenses/cddl1.txt*)

Java Architecture for XML Binding

- `jaxb-api-2.1.6.jar`

Java Mail

- `mail-1.4.jar`

JSTL

- `jstl 1.0.3.jar`

WSDL4J

Common Public License (CPL) Version 1.0. (*http://www.opensource.org/licenses/cpl1.0.php*)

- `wsdl4j-1.6.2.jar`

jQuery

- `jquery-1.4.2.js`

OpenSSL

Object-Graph Navigation Language (OGNL)

- `ognl-2.6.9.jar`

OpenSSL

Copyright © 1998-2007 The OpenSSL Project. All rights reserved. (*http://www.openssl.org/source/license.html*)

Oracle Database 10*g* JDBC Driver

Copyright © 1995-2007, Oracle. All rights reserved. (*http://www.oracle.com/*)

Spring Framework

Copyright © 2006-2008, SpringSource, All Rights Reserved. The Spring Framework is licensed under the terms of the Apache License, Version 2.0. (*http://www.springsource.org/about*)

- `spring-2.5.2.jar`
- `spring-aop-2.5.2.jar`
- `spring-beans-2.5.2.jar`
- `spring-binding-1.0.5.jar`
- `spring-context-2.5.2.jar`
- `spring-context-support-2.5.2.jar`
- `spring-core-2.5.2.jar`
- `spring-dao-2.0.8.jar`
- `spring-ibatis-2.0.8.jar`
- `spring-jdbc-2.5.2.jar`
- `spring-jms-2.5.2.jar`
- `spring-orm-2.5.2.jar`
- `spring-test-2.5.2.jar`
- `spring-tx-2.5.2.jar`
- `spring-web-2.5.2.jar`
- `spring-webflow-1.0.5.jar`
- `spring-webmvc-2.5.2.jar`
- `spring-webmvc-portlet-2.5.2.jar`
- `spring-webmvc-struts-2.5.2.jar`
- `springmodules-validation-0.4.jar`

Sun Microsystems

Copyright © 1994-2009 Sun Microsystems, Inc. All Rights Reserved.

- JavaBeans Activation Framework (JAF)
  - `activation-1.1.jar`
- Java Architecture for XML Binding (JAXB)
  - `jaxb-impl-2.1.6.jar`
- LDAP JNDI
  - `ldap-1.2.4.jar`
- JDBC
  - `jdbc-1.2.2828.jar`
- Java Servlet
  - `servlet-api-2.3.jar`
- JavaServer Pages Standard Tag Library (JSTL)
  - `jstl-1.0.3.jar`

Streaming API for XML (StAX)

- `stax-api-1.0.1.jar`

Woodstox XML Processor

- `woodstox-core-asl-3.2.0.jar`
- `woodstox-core-asl-3.2.4.jar`

XOM

- `xom-1.0.jar`

Other Trademarks

- Java™ and all Java-based trademarks are trademarks of Oracle®. in the United States, other countries, or both. Other company, product, and service names may be trademarks or service marks of others.

- WebSphere is a trademark of IBM in the United States and other countries.
- BEA WebLogic Server® is a trademarks of Oracle® in the United States and other countries.

Appendix H
Glossary

Aggregator	Third-party vendors who provides account aggregation services by collating user information across multiple enterprises.
Add-On Rule	Additional Risk Evaluation rule that ships with RiskFort.
Authentication	A process by which an entity proves that it is who it claims to be.
Callout	Custom program executing externally (outside RiskFort).
Certificate	See Digital Certificate.
Credential	A proof of user identity. Digital credentials may be stored on hardware such as smart-cards or USB tokens or on the server. They are verified during authentication.
Customer Support Representatives (CSR)	Administrators responsible for the day-to-day operations related to users of the security system. For example, Administrators can assist users with enrollment, resetting users passwords, and generating enrollment reports.
Device Velocity	Number of transactions from the same device within a specified time.
Digital Certificate	A digital document that vouches for the identity and key ownership of an individual, a computer system, or an organization. This authentication method is based on the public-key cryptography (PKI) method.
Encryption	The process of scrambling information in a way that disguises its meaning.
Exception User	User “known” to RiskFort and is excluded from risk assessments for a specified period of time.
Evaluation Callout	Callout that runs after all Evaluation Rules and contains custom risk evaluation logic.
Evaluation Rule	Pre-configured RiskFort logic that is applied to the incoming transaction data.
Extensible Element	Additional element pertaining to a transaction that is used by Add-On Rules for risk evaluation.

Global Administrator	An administrator responsible for setting up Customer Support Representatives (CSR) accounts and configuring the system.
Increased Authentication	The Risk Advice given by RiskFort, if the current transaction is considered unsafe by RiskFort. For example, if a user does a transaction of high amount for the first time. Under such circumstances, the user is asked to re-authenticate to the authentication server through stronger authentication method.
Master Administrator	The highest level of RiskFort administrator, whose primary responsibilities are to initialize RiskFort and create Global Administrator accounts.
Negative IP Address	IP address that has been the origin of known anonymizer proxies or fraudulent or malicious transactions in the past.
Negative Country	Country from which fraudulent or malicious transactions are known to have originated in the past.
Non-Terminating Rule	The rule alone does not determine overall Risk Score. It requires other rules for the purpose.
One-Way SSL	Client application verifies the identity of the server application (by accepting server's Digital Certificate) before the SSL session is established.
Private Key	One of a pair of keys used in PKI, which is kept secret and can be used to decrypt or encrypt data.
Public Key	One of a pair of keys used in PKI, which is distributed freely and is published as part of a certificate. It is typically used to encrypt data sent to the public key's owner, who then decrypts the data using the corresponding private key.
Public Key Infrastructure (PKI)	The standards and services that facilitate the use of public-key cryptography and certificates in a networked environment.
RiskFort	RiskFort provides a mechanism to evaluate the risk of a given transaction.
Risk Advice	An action (`ALLOW`, `ALERT`, `DENY`, `INCREASEAUTH`) suggested by RiskFort to the calling application, after evaluating the risk of an transaction.
RiskFort Native Protocol	Arcot proprietary protocol for communication between RiskFort Server, its components and Administration Console.

Risk Score	RiskFort announces a score depending on the evaluation result. The score can be a number from 0 through 100. The greater the number, the higher the risk.
Scoring Callout	Callout that runs after scoring by RiskFort's Scoring Engine and contains custom scoring logic to modify final Risk Score.
Scoring Engine	Component of RiskFort Server that collects Risk Scores from individual Evaluation Rules and processes them in the order of the scoring precedence.
Scoring Rule	Last Rule that receives execution results of all other configured rules and returns the final Risk Score and Risk Advice.
Server Management Protocol	Arcot proprietary protocol for starting and shutting down the RiskFort Server.
Secure Sockets Layer (SSL)	Protocol for managing the security of a message transmission on public networks.
Terminating Rule	The rule that alone determines overall Risk Score.
Transmission Control Protocol (TCP)	Internet protocol for guaranteed transmission of data. It sends data unencrypted.
Trusted Aggregator	Aggregator "trusted" to the organization and, therefore, excluded from from future risk assessments.
Trusted IP Address	IP address that is "trusted" and, therefore, excluded from future risk evaluations.
Two-Way SSL	Both, client application and the server application verify each other's identity (by presenting respective Digital Certificate) before the SSL session is established.
UserID/Password	One of the credential issued to the user during enrollment.
User Velocity	Number of transactions from the same user within a specified time.
Velocity Check	See Device Velocity and User Velocity.
Zone Hopping	Successive transactions (from same user) separated by a distance of more than what a reasonable user-speed can achieve.

Index

P

R

S

T

U