Arcot RiskFort™ Installation and Deployment Guide (for Red Hat Enterprise Linux 4.0)

Version 1.7

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot RiskFort Installation and Deployment Guide (for RHEL 4)
Version 1.7
March 2009
Part Number: ARF01-002DC-17000

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

Third Party Software

The third-party software used by Arcot RiskFort and related components are listed in "Third-Party Software Used.".

Contents

Preface

Welcome to the Arcot RiskFort Installation and Deployment Guide. This 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.

> **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",** describes the features and the architecture of RiskFort.
- **Chapter 2, "Planning the Deployment",** briefly discusses the various models that can be deployed for RiskFort and the placement of components in models.
- **Chapter 3, "Preparing for Installation",** discusses the requirements for installing RiskFort. 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.
- **Chapter 7, "Uninstalling RiskFort",** guides you through the steps for uninstalling RiskFort and related components.
- **Appendix A, "RiskFort Directory Structure",** provides the information about the location of the files that are installed by the RiskFort installer.
- **Appendix B, "Installing RiskFort with Complete WebFort Functionality",** guides you through the installation procedure, if you want to use RiskFort with a Complete installation of WebFort instead of Basic, which is typically used.
- **Appendix C, "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 D, "Database Reference",** discusses the fast-growing RiskFort tables and their trimming recommendations.
- **Appendix E, "Default Port Numbers and URLs",** lists the default port numbers and URLs that RiskFort uses.
- **Appendix F, "Third-Party Software Used",** lists the third-party software packages that are used by RiskFort.
- **Appendix G, "Glossary",** lists the key terms related to RiskFort.

Related Publication

Other related publications are as follows:

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

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Enter **Y** to accept the terms of License agreement.
Italics	Names of Publications	For more information, see the *Arcot RiskFort Administration Guide*.
	Emphasis	Sample Application must *not* be used in production deployments.
Cross reference	Links in the Guide	Refer to the section **Installing RiskFort** for more information.
`Fixed-width`	Command-Line Input or Output	`# cd /opt/oracle/`

	Text File Content	`[arcot/db/primarydb]`
		`# The name of the data source as`
		`# defined in ODBC.`
		`Datasource.1=ArcotWebFortDatabase`

	File Names	`arcotcommon.ini`

Contacting Support

If you need help, contact Arcot Support as follows:

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

Chapter 1

Understanding RiskFort

Arcot RiskFort provides real-time protection against frauds in online transactions. It gathers data during the login process to track suspicious activities and formulates a risk score and advice based on the organization's business rules and security protocols. The risk-advice then determines if the transaction is to be allowed or denied, whether a greater degree of authentication is required, or if the customer service or network security personnel need to be notified.

This chapter provides an introduction to RiskFort and its components. It covers the following topics:

RiskFort Overview

RiskFort evaluates each online transaction in real time by first examining the following data:

- Device Information (Device ID)
- Location Information (IP address, ISP, and geographical information)
- User Information (User ID)

After the required data is collected, it is forwarded to *Rules Engine* (a module of RiskFort Server). Rules Engine then evaluates this information based on default rules and historical data, if available. The evaluation result is then forwarded to another module of RiskFort Server called *Scoring Engine*.

Based on the input received from Rules Engine, Scoring Engine generates an overall *risk score*. The higher the risk score, the greater is the possibility of a transaction being fraudulent.

RiskFort then uses this risk score to generate an *Advice*. This Advice can be one of the following:

- **Allow:** RiskFort returns the Allow advice, 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 the Alert advice is returned.
- **Increase Authentication:** When RiskFort detects a suspicious transaction, it flags the transaction 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 increased authentication.
- **Deny:** RiskFort returns the Deny advice when high risk score is associated with the transaction.

RiskFort also integrates with external geo-location data repositories, such as Quova, that provides geographic information for each IP address from which a transaction originated.

> **NOTE:** You can combine RiskFort with Arcot WebFort to provide a solution that offers a strong risk-based multi-factor authentication mechanism.

RiskFort comprises of the following major components:

- **RiskFort Server**

  This is the main component that constitutes the logic for performing risk analyses. It comprises of Rule Engine and Scoring Engine. RiskFort Server stores the related information in a database, which is also referred to as **RiskFort Database.**

- **Administration Console**

  This is a Web-based console that enables you to configure RiskFort Server and its components and perform administrative tasks.

- **Risk Evaluation Java API**

  This is the Java interface between RiskFort Server and your application. It consists of the APIs that can be invoked by your application to perform risk evaluation with RiskFort Server.

- **Risk Evaluation Web Service**

  This is the Web-based interface that enables interaction over a network between RiskFort Server and your application. It consists of the Web Services that can be invoked by your Web application to perform risk evaluation with RiskFort Server.

- **Issuance Java API**

  This is the Java interface between RiskFort Server and your application. It consists of the APIs that can be invoked by your application for registering end-users in RiskFort.

- **Issuance Web Service**

  This is the Web-based interface that enables interaction over a network between RiskFort Server and your application. It consists of the Web Services that can be invoked by your Web application for registering end-users in RiskFort.

- **Machine FingerPrint (MFP) Client**

  This is the JavaScript-based RiskFort client that collects the MFP information (such as information related to Operating System, browser, user preferences, and screen settings) required for risk analyses.

Key Concepts

This section discusses the key concepts of RiskFort.

RiskFort Server

The main component of RiskFort that constitutes the logic for performing risk analyses. It comprises of Rules Engine and Scoring Engine.

RiskFort Database

RiskFort Server stores the related information in a database, which is also referred to as **RiskFort Database.**

Administration Console

This is a Web-based console that enables you to configure RiskFort Server and related administrative tasks.

Risk Evaluation SDK and Web Service

The Java or Web Services interface between RiskFort Server and your application. It consists of the APIs or Web Services that can be invoked by your application to perform risk evaluation with RiskFort Server.

Issuance SDK and Web Service

The Java or Web Services interface between RiskFort Server and your application. It consists of the APIs or Web Services that can be invoked by your application for registering end-users in RiskFort.

Sample Application

The *sample application* shipped with RiskFort is a "template" of simple primitives (code) that demonstrates the usage of RiskFort Java APIs and how your application can be integrated with RiskFort. In this manner, the sample application serves to standardize the integration process. The sample application can also be used to verify if RiskFort was installed successfully, and if is able to perform risk-evaluation operations.

Web Application

The customer Web application that uses RiskFort for real-time risk evaluation and advice.

Machine Fingerprint

The information collected by RiskFort MFP client for risk analyses. The categories of this collected information include:

- Operating system information

- Browser information
- Screen settings
- User preferences

Device ID

RiskFort uses *Device ID* to uniquely identify each user's computer. This Device ID is stored on the user's computer in form of a cookie, which can either be an HTML cookie or a Flash cookie, or both.

Rules Engine

RiskFort uses *rules* for evaluating risks. Rules are fundamental for risk evaluation because they accept input to return a score.

Rules Engine executes these rules in the order of their precedence. Eventually, it takes into account the results of different rules and derives a final risk score and advice.

Following is a list of rules that are currently pre-defined and pre-configured according to rule sets:

- **Known User**
- **Exception User**
- **Negative IP Types**
- **Negative IP Address**
- **Negative Country**
- **Trusted IP/Aggregator**
- **Device ID** Match
- **Machine Fingerprint** Match
- **User Velocity Check Rule**
- **Device Velocity Check Rule**
- **Zone Hopping Check Rule**
- **Add-On Rules**

Evaluation Rule

RiskFort Server evaluates risks by using evaluation rules. An *evaluation rule* uses a pre-configured logic which is applied to the incoming transaction data. Each rule has an associated risk-score, which is returned if the rule-logic matches.

Rules Engine sequences and processes the rules based on the group information, credential type, and action.

Scoring Engine

Scoring Engine collects risk-scores from individual rules and processes them in the order of the scoring precedence of the rules. Eventually, it generates a final *risk score* and advice.

Risk Advice

The risk score is an integer through 0 to 100. The score is then converted into a recommended *risk advice* by using a Risk Advice Matrix.

The following table shows a sample Risk Advice Matrix.

Table 1-1 Risk Advice Matrix

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

Known 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. Such a user is referred to as an *exception user*. RiskFort returns a low risk score for transactions originating from exception users.

For example, if exception users travel to a negative country, then RiskFort will process their transactions with a low risk score so that those transactions are allowed.

Negative IP Types

Negative IP type list comprises the categories that a negative IP can be classified as. These include:

- Negative
- Active
- Suspect
- Private
- Inactive
- Unknown

See the "Configuring Negative IP Types" section in the *RiskFort Administration Guide* for more information on how configure negative IP address list.

Negative IP Address

Negative IP addresses constitute IP addresses that originate from anonymizer proxies or have been the origin of known fraudulent or malicious transactions in the past. RiskFort matches the IP address of a transaction against the list of negative IPs during the risk evaluation process.

The negative IP address list consists of both unique IP address and IP ranges. RiskFort Administration Console is used to configure the list of negative IPs.

See the "Configuring Negative IP Address" section in the *RiskFort Administration Guide* for more information on how configure negative IP address list.

Negative Country

Negative country configuration comprises a list of countries that have been known to be origins of significant number of frauds in the past. Organizational policies can prohibit transactions originating from such countries.

The list of negative countries is configurable by using the RiskFort Administration Console. 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.

RiskFort integrates with Quova (`http://www.quova.com`) for obtaining detailed geographic information for each IP address.

See the "Configuring Negative Country List" section in the *RiskFort Administration Guide* for information on how configure negative country list.

Trusted IP/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 need to be excluded from risk assessment. To realize this, RiskFort provides the ability to configure a *Trusted Aggregator* list so that all transactions originating from the aggregator’s IP addresses are assigned a low risk-score.

An aggregator’s IP is uniquely identified by RiskFort by using a combination of IP range and AggregatorID. RiskFort looks for this IP address and ID in incoming transactions to determine if the transaction is from a trusted aggregator or not.Using RiskFort Administration Console, one AggregatorID is issued for each “trusted” Aggregator.

Transactions routed through the trusted account-aggregation provider receive a low score and the advice is `Allow`.

See the "Configuring Trusted Aggregators" section in the *RiskFort Administration Guide* for information on how to configure trusted aggregators.

What's New in this Release

This section provides a quick glance at the new features and enhancements in:

- RiskFort 1.7

RiskFort 1.7

The new features and enhancements introduced in RiskFort release **1.7** are:

> **NOTE:** Most of these features are available through the Administration Console. Refer to *Arcot RiskFort Administration Guide* for more information on these features.

- **Flexible Scoring Configurations**

  Administrators can now enable or disable rules, change the priority of scoring rules, and configure the risk scores for each rule by using the Administration Console.

- **User Velocity Check Rule**

  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. Administrators can now configure RiskFort to track for this behavior.

- **Device Velocity Check Rule**

  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.

- **Zone Hopping Check Rule**

  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 such cases, administrators can use RiskFort to configure and track this behavior.

  RiskFort can also be configured for **sharing a User ID**, 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.

- **Trusted IP Support**

  In addition to existing feature of Trusted Aggregator, RiskFort can also be configured to allow transactions from specified IP addresses and ranges.

- **Negative IP Rule Enhancement**

  Administrators can now configure negative IP addresses by using the Administration Console. Also, RiskFort now leverages Quova's Anonymizer data for negative IPs. In addition, the corresponding negative IP report has also been enhanced to support this change.

- **Add-On Rules**

  RiskFort now ships with the ability to handle custom rules that can be configured and deployed based on your organization's requirements. These rules execute like any other evaluation rule, but *after* the execution of all out-of-box evaluation rules. However, you can change their scoring priority by using the Administration Console.

  A new column also has been added in **Audit Log Reports** to display the result of Add-on Rules. This column displays the results of all Add-On rules as one field, separated by a delimiter.

- **Evaluation (HTTP) CallOuts**

  The available RiskFort risk evaluation functionality can be extended by using custom logic to collect information from other risk assessment systems.

  RiskFort provides infrastructure for posting `HTTP` data to an external system, which specifies whether a custom rule matched or not. This result is then used by RiskFort to determine the Risk Score and Advice for the transaction.

- **Scoring (HTTP) CallOuts**

  The available RiskFort risk scoring functionality can also be extended by using custom logic to collect information from other risk assessment systems.

  RiskFort provides infrastructure for posting `HTTP` data to an external system, which can respond with its own Risk Score. RiskFort then converts this Score to a corresponding Advice.

- **Extensible Elements**

  RiskFort now supports an extensible set of elements for supporting custom Callouts and Add-On Rules.

- **Tool to Upload GeoPoint and Anonymizer Data**

  This release provides **Arcot RiskFort Data Upload Tool** for uploading Quova data to RiskFort.

- **Support for all Language Characters in User Name, Association Name, and Group Name**

  RiskFort now accepts characters in all languages in user name, association name, and group name. RiskFort only prohibits the following characters that are deemed to make Web applications vulnerable:

  - **User Name:** All whitespace characters (ASCII 0 - 32) and:

    `# * / \ ? | " < > : , = ( )`

  - **Association Name:** Whitespace characters (ASCII 0-31) *except* Space and:

    `< > : , = ( )`

  - **Transaction Type:** Whitespace characters (ASCII 0-31)*except* Space and:

    `< > : , = ( )`

- **New Admin Web Service APIs**

  New Web service APIs that can be integrated into your existing Administration Console. These APIs provide transaction details, enable operations for managing Exception users (such as creating and removing users from Exception List), and provide the capability to mark a transaction as "Fraud" to support Case Management.

- **Serializable evaluateRisk() Response**

  RiskFort Java-based `evaluateRisk` APIs have been enhanced to return Serializable `evaluateRisk Response` object.

- **Implicit User Creation**

  A user must exist in the RiskFort database for subsequent risk evaluations. Otherwise, RiskFort will treat them as a first-time user and will generate the `ALERT` risk advice. Earlier, a user could only be created in the RiskFort Database by making an explicit User Creation (`createUser()` call).

  RiskFort now can be configured to create users implicitly during risk evaluation (the `evaluateRisk()` call), if the user does not already exist in RiskFort database.

- **Configurable Machine FingerPrint (MFP) Threshold Percentage**

  RiskFort can now be configured for the percentage match of MFP that should be considered a successful match. By default if the MFP of the incoming request matches more than 50% with that of the MFP stored for the device, then it is considered a successful match.

- **New Issuance Java SDK and Web Service**

  The new Issuance SDK and Web Service now directly communicates with the RiskFort Server and not the RiskFort Database, as in previous releases. Also, this new Issuance API has no dependency on JNI, which makes it easier to deploy.

- **Support for Transaction Type**

  RiskFort APIs have been enhanced to accept **transaction type** as an input.

- **Updated Timeout Units in Properties Files**

  The unit of all timeout parameter values in all properties files have been updated to timeouts.

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 an overview of steps for deploying RiskFort and provides pointers for choosing a deployment model based on your requirements.

The following is an overview of the steps for deploying RiskFort so that it can perform risk evaluation-related tasks:

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. Install all prerequisite software.

   See **"System Requirements"** for more information.

3. Create a database user in the SQL database.

   See **"Configuring Database Server"** for more information.

4. Install RiskFort:

   - See **"Deploying RiskFort On a Single System"** for more information on installing in a single-system environment.
   - See **"Deploying RiskFort on a Distributed System"** for more information on installing in a distributed environment.

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

   - See **"Running Database Scripts"** for more information on running SQL scripts for single-system deployment.
   - See **"Running Database Scripts"** for more information on running SQL scripts for distributed deployment.

6. Deploy and start the Administration Console:

   - See **"Deploying Administration Console"** for more information on deploying and starting Administration Console for single-system deployment.
   - See **"Deploying Administration Console"** for more information on deploying and starting Administration Console for distributed deployment.

7. Create a Global Administrator account for setting additional configuration values:

- See "Creating a Global Administrator" for more information on doing this in a single-system environment.
- See "Creating a Global Administrator" for more information on doing this in a distributed environment.

8. Deploy and run the Sample Application to test RiskFort installation:
   - See "Deploying Sample Application","Configuring Sample Application for Communication with RiskFort Server", and "Using Sample Application" for more information on doing this in a single-system environment.
   - See "Deploying Sample Application", "Configuring Sample Application for Communication with RiskFort Server", and "Using Sample Application" 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 and session 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" 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: Install a database server on the system which has RiskFort Server, or use an existing database on a separate system.

Decision: Use Sample Application or write your own Web application.

> **NOTE:** 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.

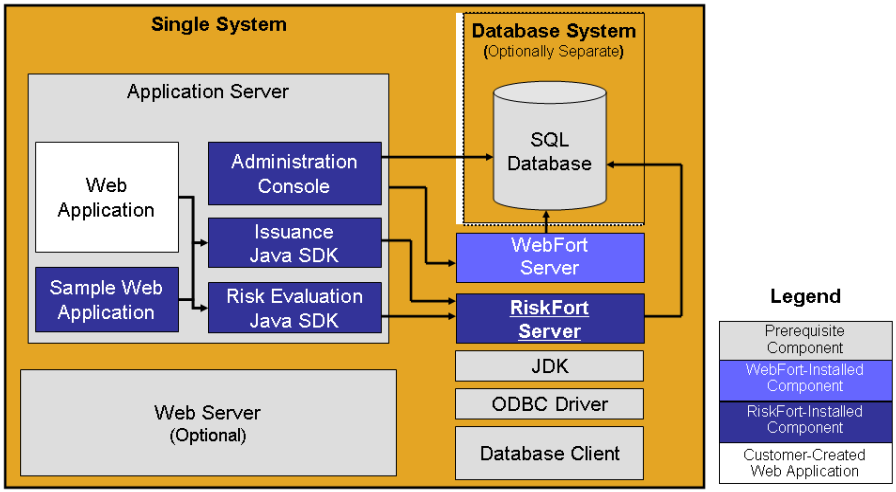
Decision: Use Java SDKs or Web Services to integrate with your own Web application.

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

Deploying Java SDKs

The following figure illustrates RiskFort Server and Java SDKs deployed on a single system.

Figure 2-1

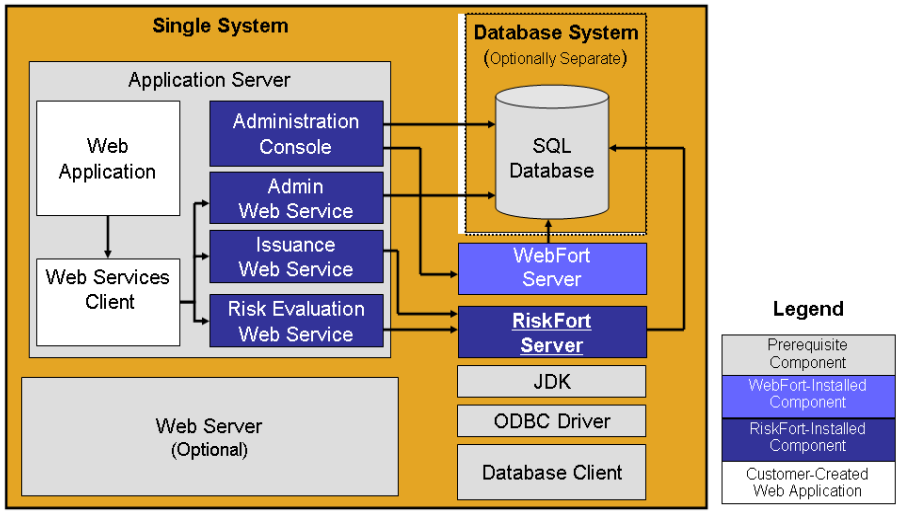


NOTE: The use of a Web server to deliver HTML pages for the application server is optional and is transparent to RiskFort. In production deployments, this approach is generally used to improve Application Server performance and security. Refer to the documentation of your Application Server for detailed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

Deploying Web Services

The following figure illustrates RiskFort Server and Web Services on a single system.

Figure 2-2



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" 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

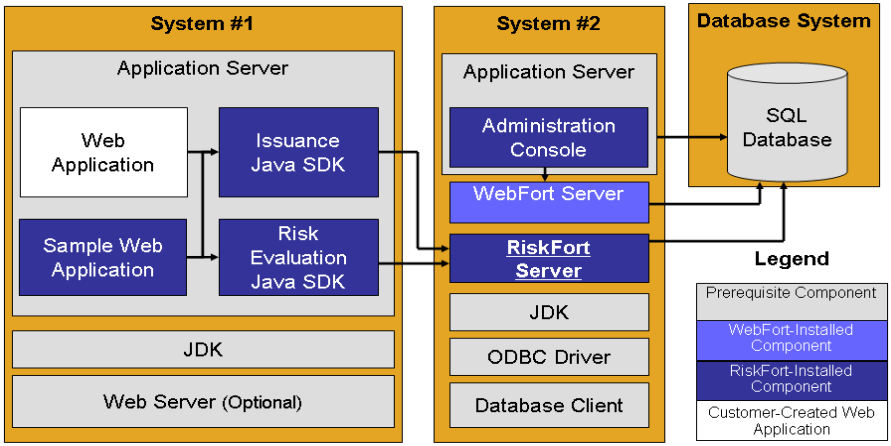
The diagrams in this section depict several possible options, where prerequisites and RiskFort components can be installed on multiple systems:

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

Deploying Single Application with Java SDKs

The following illustrates RiskFort using Java SDKs with a single application.

Figure 2-3

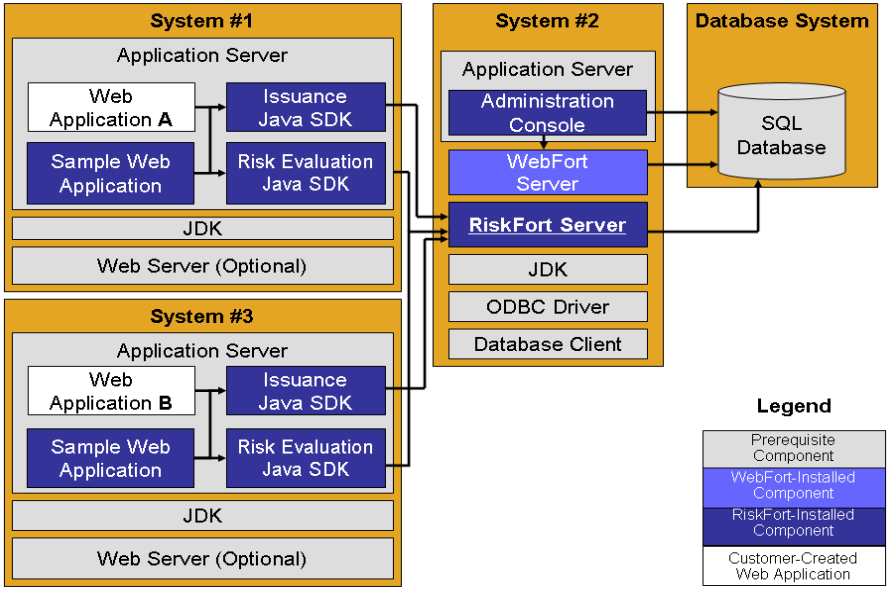


NOTE: The Administration Console can be installed on any individual system, every system, or on a system not listed in the diagrams.

Deploying Multiple Applications with Java SDKs

The following figure illustrates RiskFort deployment using Java SDK with multiple applications.

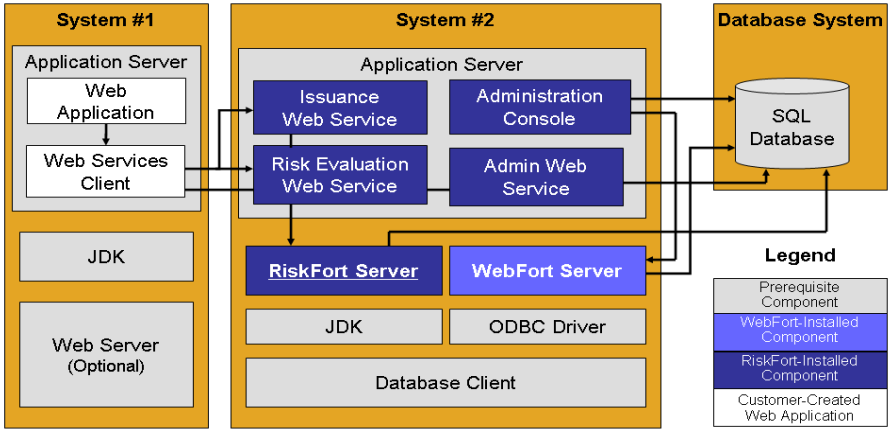
Figure 2-4



Deploying Single Application with Web Services

The following figure illustrates RiskFort deployment using Web Services on a single application.

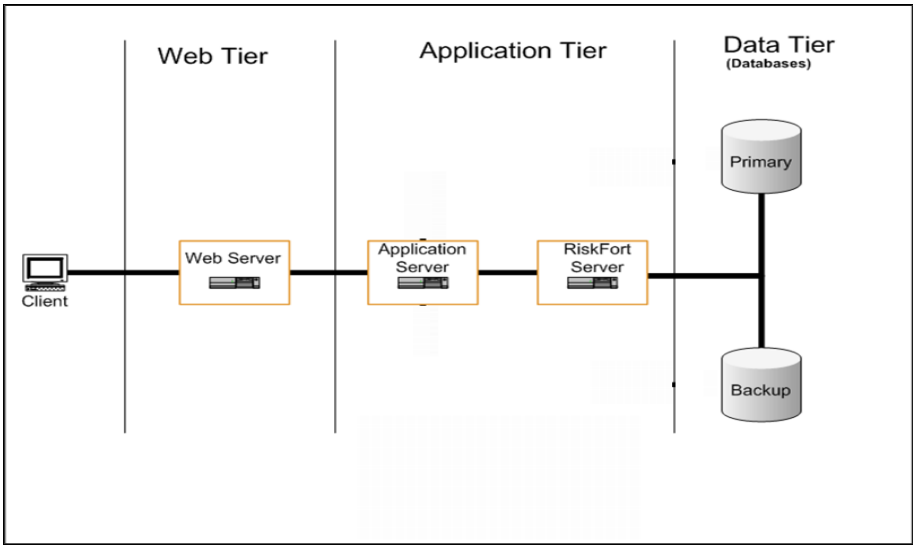
Figure 2-5



Architecture Diagram

The following figure shows the architecture diagram for a distributed-system deployment.

Figure 2-6 .



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
- Architecture Diagram

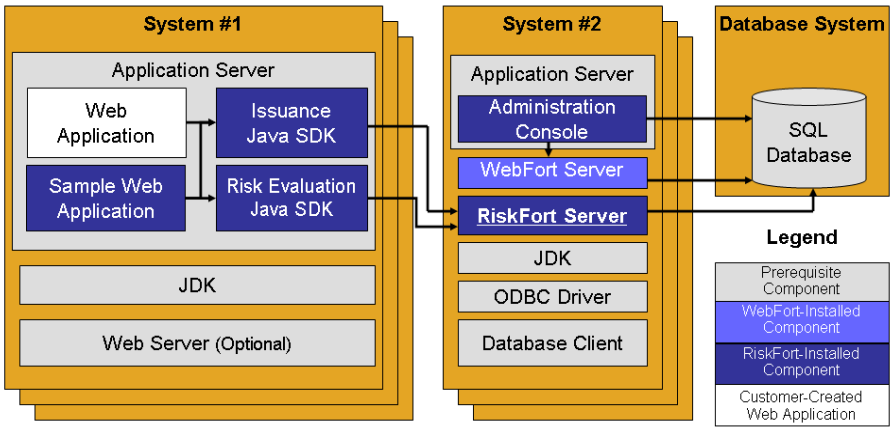
Component Diagrams

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

The following figure illustrates multiple-instance deployment of RiskFort using Java SDK.

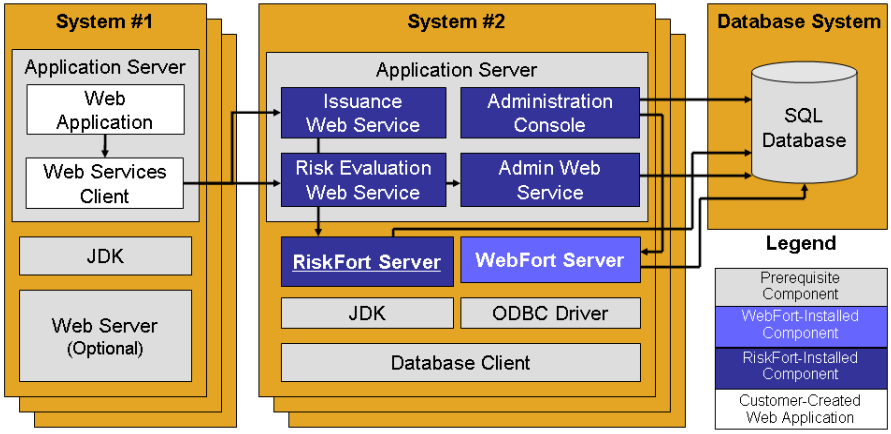
Figure 2-7



High-Availability Deployment Using Web Services

The following figure illustrates multiple-instance deployment of RiskFort using Web Services.

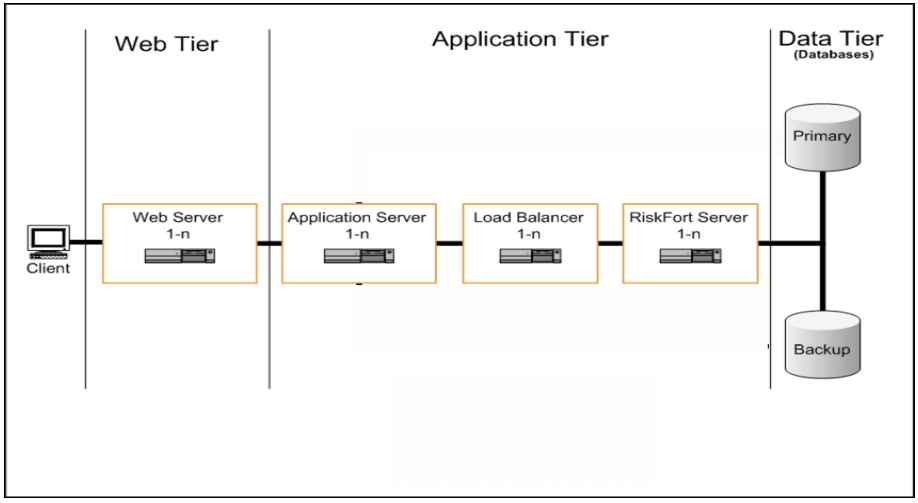
Figure 2-8



Architecture Diagram

The following figure shows the architecture diagram for a multiple-instance deployment.

Figure 2-9



Chapter 3

Preparing for Installation

Before installing RiskFort, 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:

System Requirements

The computer where you plan to install all or any components of RiskFort must meet the following requirements:

- Hardware Requirements
- Software Requirements

Hardware Requirements

The following are the *minimum* hardware requirements for installing RiskFort:

- Requirements for RiskFort with database on single system:
  - **RAM:** 1 GB
  - **Hard Drive Space:** 10 GB
  - **Processor:** 2.4 GHz
- Requirements for RiskFort with database on a different system:
  - **RAM:** 512 MB
  - **Hard Drive Space:** 300 MB
  - **Processor:** 2.4 GHz Ultra

    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

This section lists the supported software for Red Hat Enterprise Linux 4.0 on 32-bit and 64-bit platforms. The following information for software requirement is provided in this section:

- Prerequisites for RiskFort Components
- Minimum Software Requirements
- Locations for Downloading Prerequisite Software

Prerequisites for RiskFort Components

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.

The following table indicates the prerequisite software required by each RiskFort component.

Table 3-1 Prerequisites for RiskFort Components

Component \ Prerequisite	Database Client	ODBC Driver	JDK	Application Server
RiskFort Server	✓	✓		
Administration Console			✓	✓
RiskFort Java SDK			✓	✓
Issuance Java SDK			✓	✓
RiskFort Web Service			✓	✓
Issuance Web Service			✓	✓
Sample Application			✓	✓

Minimum Software Requirements

This section lists the supported software for the following versions of Red Hat Enterprise Linux 4 (x86):

- Red Hat Enterprise Linux 4 (32-Bit) on x-86 Platform

Red Hat Enterprise Linux 4 (32-Bit) on x-86 Platform

This section lists the following software requirements that your computer must meet for installing RiskFort successfully on RHEL 4 (32-bit) on x-86 platforms:

- Database Requirements
- JDK and Application Server Requirements

Database Requirements

Table 3-2 lists all the supported software required for the Database that is used by RiskFort for RHEL 4 (32-bit) on x86 platforms.

Table 3-2 Database Requirements for RHEL 4 (x86 32-Bit)

Supported Platform	Database Server	Database Client	ODBC Driver
Red Hat Enterprise Linux 4 (x86 32-bit)	Oracle 10*g*	Oracle 10*g*	Arcot Branded DataDirect ODBC Driver 05.20.0048 (Oracle Client Protocol)

JDK and Application Server Requirements

Table 3-3 lists the version of JDK and application server supported by RiskFort for RHEL 4 (32-bit) on x86 platforms.

Table 3-3 JDK and Application Server Requirements for RHEL 4 (x86 32-Bit)

Supported Platform	Sun JDK	Application Server
Red Hat Enterprise Linux 4 (x86 32-bit)	1.5.0_10	Tomcat 5.5.23

Locations for Downloading Prerequisite Software

The following list provides the location for downloading the prerequisite software:

1. **Sun JDK Archive Downloads (for 1.5)**

   `http://java.sun.com/products/archive/`

2. **Sun JDK 5.0** (use the plain JDK, NetBeans or EE are not required)

   `http://java.sun.com/javase/downloads/index_jdk5.jsp`

3. **Apache Tomcat 5.5.23** (`5.5.23.tar.gz`)

   `http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.23/bin/`

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 (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. In addition, the database server and the system that has the Arcot products installed ***must*** have the same time-zone setting.

Configuring Oracle Database

There are specific configuration requirements for Oracle Database Server. 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.

> **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-initial-config-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-initial-config-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:

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

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 D, "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` and `CREATE TABLE` privileges.
5. Grant the user `ALTER EXTENT PARAMETERS` privilege.
6. 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 (and the Database Client, in case of Oracle Database Server) 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:

Oracle Database Post-Installation Tasks

Perform the following steps before you install RiskFort. You will need this information when you install RiskFort:

1. Get the following database information from the DBA:

   a. **TNS Service Name** (Use of `arcotdbtns` is recommended)

   b. **Service ID** (Instance identifier of the Oracle database)

   c. **Host Name**

   d. **Port Number**

   e. **User Name**

   f. **Password**

   Refer to Step 14 on page 39 for more information on these parameters.

2. **Install Oracle Client.**

   Install Oracle Database Client if a supported version is not already installed. You can run the installer with **Admin** option.

   At the end of the installation, you will be prompted to set up the TNS Name for the database. Refer to the information provided by the DBA (Step 1).

3. **Set up TNS Names.**

If Oracle Database Client is already installed, run the **Net Configuration Assistant** to configure the `tnsnames.ora` file with the database that RiskFort will be accessing. The recommended name is `arcotdbtns`.

The `tnsnames.ora` file allows RiskFort to reference the Oracle databases by their alias.

4. **Install Arcot-branded Oracle ODBC Driver.**

   To set up the Arcot-branded Data Direct ODBC driver to work with RiskFort, perform the following steps:

   a. Log in and navigate to the `Arcot-RiskFort-1.7-Linux/Misc/` directory.

   b. Unzip the ODBC driver GZIP file, shipped with the package as follows:

      ```
      prompt> gzip -d odbc32v52wf.tar.gz
      ```

   c. Extract the resultant TAR file as follows:

      I. Copy the `odbc32v52wf.tar` file to the `/opt` directory.

         ```
         prompt> cp odbc32v52wf.tar /opt
         ```

      II. Change to the `/opt` directory.

         ```
         prompt> cd /opt
         ```

      III. Extract the content of the TAR file.

         ```
         prompt> tar -xvf odbc32v52wf.tar
         ```

Requirements for Java-Dependent Components

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

- **JDK**
- **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.

  IMPORTANT: If you are using Apache Tomcat application server, then ensure the `JAVA_HOME` points to `javac` and that `JRE_HOME` points to `java`.

Chapter 4

Deploying RiskFort On a Single System

Use the **Arcot RiskFort 1.7 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 "Running Database Scripts" and "Verifying the Database Setup" for more information.

3. Deploy Administration Console in the application server and verify the deployment.

   See "Deploying Administration Console" and "Verifying the Administration Console Deployment" for more information.

4. Log in to Administration Console with the Master Administrator credentials to initialize RiskFort and then create a Global Administrator.

   See "Logging in to Administration Console" and "Creating a Global Administrator" for more information.

5. To ensure secure communication between RiskFort components, you can configure them to support TLS (Transport Layer Security) transport mode. This is an optional step.

   See "(Optional) Configuring TLS Communication Mode" for more information.

6. 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.

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 1.7 does not support upgrade from a previous version (1.6.1 or earlier). Also, you can not install RiskFort 1.7 over a previously installed version.
- Currently, you can not modify or repair RiskFort components by using the installer. You *must* uninstall the component and then re-install it.
- The installation directory name that you specify *must not* contain any spaces. If there are spaces in the installation directory name, some of the RiskFort scripts might not function as intended.
- Any time during the installation, you can type `quit` and press **Enter** to exit the installation.

Performing Complete Installation

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.

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. Log in and navigate to the location where `Arcot-RiskFort-1.7-Linux.tar.gz` is located.
2. Uncompress and untar the installer.
3. Navigate to the directory where you untarred the installer.
4. Run the installer as follows:

   ```
   prompt>sh Arcot-RiskFort-1.7-Linux-Installer.bin
   ```

   If you are executing the installer with `root` login, then a warning message appears. Enter **Y** to continue, or enter **N** to quit the installation.

   If you exit the installer screen, then you must run the installer again.

5. Press **Enter** to continue.

   The Welcome screen appears.

6. Press **Enter** to continue with the installation.

   The License Agreement for RiskFort appears.

7. On the License Agreement screen:

   a. Read the text carefully and press **Enter** to display the next screen of the license text. You might have to press **Enter** multiple times, until the entire text for License Agreement is displayed.

      At the end of the license agreement, you will be prompted for acceptance of the terms of license agreement.

   b. Enter **y** to accept the acceptance of License Agreement and to continue with the installation.

NOTE: If you press **n**, then a warning message will be displayed and the installation will be aborted.

The Choose Installation Location screen appears.

8. As directed on the screen, you can *either*:

   - Enter the absolute path of the directory where you want to install RiskFort and press **Enter** to continue.

     NOTE: The installation directory name that you specify *must not* contain any spaces. Else, some RiskFort scripts and tools might not function as intended.

   - Press **Enter** to accept the default directory displayed by the installer.

   The installer displays the installation options supported by RiskFort.

   If the computer where you are currently performing the installation already has an existing Arcot product installed, then the installer displays the following options:

   - **1** - Enter a new location.
   - **2** - Continue to install in the directory selected in **Step 8**.
   - **3** - Use the location at which the existing Arcot product is installed.

9. Select the required option and press **Enter** to continue with the installation.

   NOTE: If you selected option 1 or 2, then a new directory called `arcot` will be created in the specified location.

   The Choose Install Type of Installation screen appears. This screen displays the installation types (Complete and Custom) supported by RiskFort.

10. Enter **1** to select the default (**Complete**) option and install all components of RiskFort.

    The ODBC Home Configuration screen appears. This screen prompts you to specify the path to the ODBC Driver.

11. Enter the absolute search path (for example, `/opt`) where the ODBC driver for the database is available, and press **Enter** to continue.

    The installer checks for the ODBC drivers present in the specified location. If multiple versions are found, then the installer displays all versions and prompts you to select one. If no ODBC driver is found in the specified location, then you are prompted for another location.

    The Oracle Home Configuration screen appears. This screen prompts you to specify the Oracle Client path.

12. Enter the absolute search path where Oracle Client is available, and press **Enter** to continue.

    The installer checks for Oracle Client in the specified location. If multiple entries are found, then the installer displays all of them and prompts you to select one. If no Oracle Client is found in the specified location, then you are prompted for another location.

    The Java Home Configuration screen appears.

13. Enter the absolute search path for JAVA HOME and press **Enter** to continue.

    The installer checks for `JAVA HOME` in the specified location. If multiple versions are found, then the installer displays all and prompts you to select one. If no `JAVA HOME` is found in the specified location, then you are prompted for another location.

    The Primary Database Access Configuration screen appears.

14. On the Primary Database Access Configuration screen:

    a. Specify the name of the DSN, when prompted, and press **Enter.**

       The installer checks for the availability of the specified DSN. If this DSN is already present, then appropriate messages are displayed.

    b. Specify the appropriate choice (**1**, **2**, or **3**) and press **Enter** to continue.

       The installer now prompts you for more information related to the specified DSN.

c. Specify the information listed in the following table.

Table 4-1 Primary DSN Parameters

Parameter	Description
TNS Service Name	Transparent Network Substrate (TNS) is used by Oracle databases and specifies the name by which an Oracle database instance is known on a network. In other words, TNS Name resolves to the protocol, IP, port, and SID of an oracle database. The name can be found in the `tnsnames.ora` file on the local system.
User Name	The database user name for RiskFort to access the database. This name is specified by the database administrator. **NOTE:** The User Name 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.
SID	The Oracle System Identifier (SID) that refers to the instance of the Oracle database running on the server.
Port No	The port at which the Database listens to the incoming requests.
Host Name	The host name or IP address of the RiskFort datastore. **Syntax**: *<server_name>* **Example**: `demodatabase`

d. Enter **Y** to test connectivity to the specified database, or **N** to skip this test.

The Backup Database Access Configuration screen appears.

15. On the Backup Database Access Configuration screen:

- Type **N** to skip the configuration of the secondary DSN, when prompted, and press **Enter** to continue to the next screen.
- Type **Y** to configure the secondary DSN, when prompted, and press **Enter** to continue.

  See the sub-steps of **Step 14** for more information on the tasks to be performed.

The WebFort Connectivity screen appears.

16. Specify the Host Name and the Port number of WebFort Server and press **Enter** to continue. This information is required by Administration Console to connect to WebFort and authenticate the RiskFort administrators.

    The Pre-Installation Summary screen appears. This screen lists the product details, installation directory, type of installation, components that are to be installed, and disk space-related information.

17. Review the product details displayed carefully and press **Enter** to proceed with the installation. If you would like to change a configuration on any of the previous screens, type **back** until you reach the screen, make the required changes, and press **Enter** to proceed to the next screen.

    The Installing screen appears. This might take several minutes, because the installer now:

    - Puts all the components and their related binaries in the installation directory.
    - Stores database settings in the **arcotcommon.ini** file and the password in the `securestore.enc` file.
    - Writes to the required INI files.
    - Sets the environment variables such as, `JNI_LIBRARY_PATH` for Issuance and Administration Console and `ODBC_HOME`, `ODBCINI`, `ORACLE_HOME`, and `ORACLE_LIB_PATH` in the `arctenv` file.
    - Creates or overwrites, as specified in a previous screen, the Primary DSN and Backup DSN (if selected and configured) using the selected ODBC driver in the `odbc.ini` file.

    After the preceding tasks are completed successfully, the Installation Complete screen appears.

18. Press **Enter** to exit the installer.

    You might have to wait for a few minutes (for the installer to clean up temporary files) until the prompt re-appears.

19. Check the installation log file, which is available in the `<install_location>/arcot/` directory.

20. Perform **WebFort Basic Installation**:

    a. Navigate to the directory where the `Arcot-WebFort-5.4.1-Linux.tar.gz` file is located.

    b. Gunzip and untar the file, and then run the installation wizard, as follows:

```
prompt> sh Arcot-WebFort-5.4.1-Linux-Installer.bin
```

c. Follow the instructions on the following screens to install. On the Type of Installation screen, you must enter **2** to specify the **Basic** option.

See the *Arcot WebFort Installation and Deployment Guide* for detailed instructions to perform WebFort Basic 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 in the following directory:

`<install_location>/arcot/`

If for some reason, the installation failed, then the error log is available in the `/tmp` directory.

WebFort Basic Installation

The Administration Console is a common component included in many Arcot products. It uses WebFort Server to authenticate users when they log in. As a result, WebFort is a required component for other Arcot products, including RiskFort.

However, WebFort Basic is *not* packaged as a part of RiskFort. To configure Administration Console to access WebFort, it is highly recommended that you perform **Basic** installation of WebFort *after* completing the installation of RiskFort. The Basic deployment installs only WebFort Server.

NOTE: Refer to the *Arcot WebFort Installation and Deployment Guide* for detailed steps for performing WebFort **Basic** installation.

While performing WebFort **Basic** installation, if the corresponding RiskFort DSN configuration has already been completed, then you will not be prompted for the DSN-related information. However, if the DSN has not already been configured, then you will need to specify this information in the additional screens that appear.

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. Running Database Scripts
2. Verifying the Database Setup
3. Verifying the Installation
4. Deploying Administration Console
5. Verifying the Administration Console Deployment
6. Logging in to Administration Console
7. Creating a Global Administrator
8. (Optional) Configuring TLS Communication Mode
9. Deploying Sample Application
10. Configuring Sample Application for Communication with RiskFort Server
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".

Running Database Scripts

> **NOTE:** 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" 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/dbscripts/oracle/`

2. Run the scripts *in the following order*:

- `arcot-db-initial-config-common-1.0.sql`
- `arcot-db-config-for-webfort-5.4.1.sql`
- `arcot-db-config-for-riskfort-1.7.sql`

Verifying the Database Setup

After the database has been set up, you must verify whether the database was set up correctly. To do so, perform the following tasks:

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

```
SELECT SERVERNAME, VERSION FROM ARSERVERS;
```

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

```
SERVERNAME                VERSION
------------------------  ----------------
WebFort                     5.4.1
RiskFort                    1.7
Admin Console               5.4.1
WebFort Issuance            5.4.1
```

3. Log out of the database console.

Verifying the Installation

After you have run the database scripts (mentioned in the **"Running Database Scripts"** section) to create the required tables, you must verify whether RiskFort was installed correctly. Perform the following tasks to do so:

1. **Starting RiskFort Server**
2. **Verifying the Log Files**

Starting RiskFort Server

Perform the following steps to start the RiskFort Server:

1. Navigate to the following directory:

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

2. Run the following commands:

```
./webfortserver start
./riskfortserver start
```

After starting the server, you must check if the server started successfully. To do so:

1. Navigate to the following directory:

   `<install_location>/arcot/logs/`

2. Open the `arcotriskfort.log` file by using any editor.
3. Locate the following line in the file:

```
Arcot RiskFort Service READY
```

Stopping the RiskFort Server

If at any time, you want to stop the RiskFort or WebFort Server, then perform the following steps to do so:

Perform the following steps to start the RiskFort and WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following commands:

   - `./riskfortserver stop [server_ip_address] [server_management_port_number]`

     The default value for *server_management_port_number* is `7980`. This is a configurable value.

   - `./webfortserver stop [server_ip_address] [server_management_port_number]`

     The default value for *server_management_port_number* is `9743`. This is a configurable value.

Verifying the Log Files

The two log files that you need to verify if the RiskFort and WebFort servers started correctly are:

- `arcotriskfort.log`
- `arcotwebfort.log`

Perform the following steps to verify if the servers started correctly:

1. Navigate to the following location:

   `<install_location>/arcot/logs/`

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

   - `STARTING Arcot RiskFort 1.7.0_1`

     This is the first line in the file.

   - `Arcot RiskFort Service READY`

     This is the last line in the file.

3. Open the `arcotwebfort.log` file in any editor and locate the following lines:

   - `STARTING Arcot WebFort 5.4.1_1`

     This is the first line in the file.

   - `Arcot WebFort Authentication Service READY`

     This is the last line in the file.

     NOTE: You might also want to make sure that the log files do not contain any FATAL messages.

Deploying Administration Console

The Administration Console is a browser-based interface to RiskFort that enables you to customize the server configurations, if required.

> **NOTE:** Arcot strongly recommends that you configure the Administration Console *after* you have completed the **Basic** WebFort installation. Refer to the *Arcot WebFort Installation and Deployment Guide* for detailed steps for performing WebFort Basic installation.

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

`<install_location>/arcot/java/app/admin/`

To deploy the WAR file on your application server:

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

   The deployment directory and procedure will depend on the application server that you are using. Refer to your Application server documentation for detailed instructions.

   For example, in case of Apache Tomcat, you must deploy the `arcotadmin.war` file in the following location:

   `<APP_SERVER_HOME>/webapps/`

2. Navigate to the `<install_location>/arcot/sbin/` directory.
3. Run the following command to set the required environment variables:

   ```
   . ./arctenv
   ```

4. Start the application server.

Verifying the Administration Console Deployment

The `arcotadmin.log` file is used for logging the Administration Console information. This file is available in the `<APP_SERVER_HOME>` of your application server.

After you deploy the Administration Console successfully, navigate to the `arcotadmin.log` file, open it any editor, and locate the following lines:

- `Title: Arcot Admin Console, Vendor: Arcot Systems Inc., Version No:5.4.1`
- `Servlet 'cygnetadmin' configured successfully`

These lines indicate that your Administration Console was deployed successfully.

Changing the Default Log File Location

By default, the log files for Administration Console are generated in the default log directory of your application server. However, you might want to specify a different directory to store the log files for Administration Console. In this case, perform the following steps:

1. Navigate to the `<APP_SERVER_HOME>` directory.
2. Navigate to the subdirectory where the `log4j.properties` file is located.
3. Open the `log4j.properties` file in any editor window.

4. Locate the `log4j.appender.debuglog.File` property and specify the absolute file path to the `arcotadmin.log` file as its value.

   For example:

   `log4j.appender.debuglog.File=<install_location>/arcot/logs/arcotadmin.log`

5. Restart application server for the change to take effect.

Logging in to Administration Console

> **NOTE:** You *must* start the RiskFort and WebFort servers before attempting to log in into Administration Console application.

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

To log in to the Administration Console:

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

   `http://<host>:<port>/arcotadmin/adminlogin.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:** Master_Admin
   - **Password:** master1234

     > **NOTE:** 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.

Creating a Global Administrator

When you install and configure RiskFort, the *Master Administrator* account is created by default. However, this account can only perform restricted activities, such as initializing the system and creating the next level of administrators, called Global Administrator. For any advanced configurations, you must now create at least one Global Administrator account.

Global Administrators are responsible for configuring the global settings and setting up the communication protocol. They can also create next level of administrators and manage their credentials.

> **NOTE:** Refer to *Arcot RiskFort Administration Guide* for more information on Global administrator privileges.

To create a Global Administrator account:

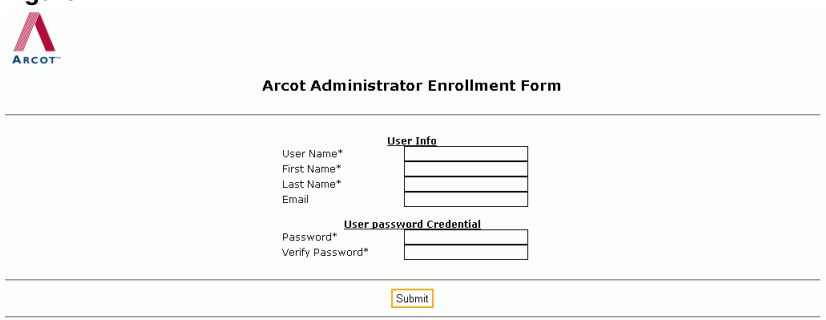
1. Access the Administration Console by using the following URL:

   `http://<host>:<port>/arcotadmin/adminlogin.htm`

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

   The Arcot Administrator Enrollment Form page, as shown in following figure, appears.

Figure 4-1



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

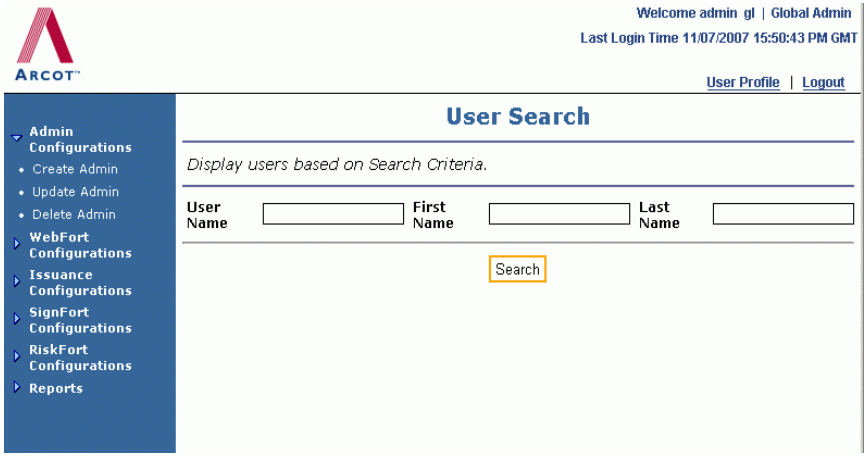
   > **NOTE:** Fields marked with * are mandatory fields. The field **User Name** is not case sensitive.

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

4. Log in as Master Administrator again.
5. Under **Admin Configurations**, select the **Create Admin** option.

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

Figure 4-2

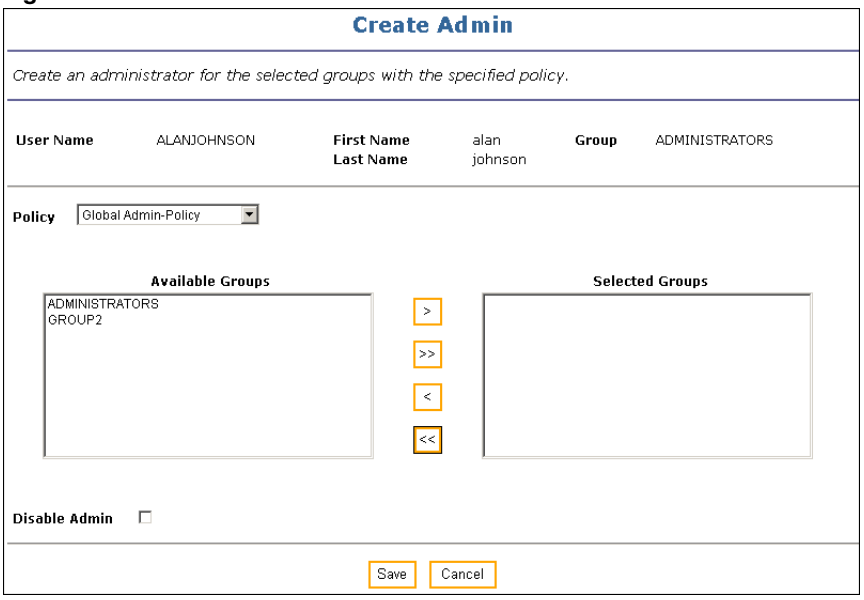


6. Provide complete or partial details of the user and click the **Search** button.

   A list of enrolled users matching the search criteria and who are not administrators is displayed.
7. Click the **User Name** link for the user you want to promote as an administrator.

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

Figure 4-3



8. To specify the level of the administrator, you must select the policy to be associated. Select the **Global Admin-Policy** option from the **Policy** drop-down list.

9. Select the group from the **Available Groups** list and click the > button to add the group to the **Selected Groups** list.

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

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

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

    The "Admin created successfully" message appears.

(Optional) Configuring TLS Communication Mode

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 WebFort Server and between SDKs and RiskFort Server, you can configure RiskFort Native and Server Management protocols to support TLS (Transport Layer Security), which ensures securer communication between applications across insecure media and reduces the chances of TCP attacks.

This section discusses the steps to configure TLS-based communication:

- **Between WebFort Server and Administration Console**
- **Between RiskFort Server and Java SDKs**
- **Between RiskFort Server and Web Services**

Between WebFort Server and Administration Console

By default, Administration Console uses Transmission Control Protocol (TCP) to communicate with WebFort Server. See "WebFort Basic Installation" for more information.

To enable TLS communication between WebFort Server and Java SDKs, you must first configure the WebFort Native protocol settings by using the Administration Console and then configure the **`adminserver.ini`** file, which is available at:

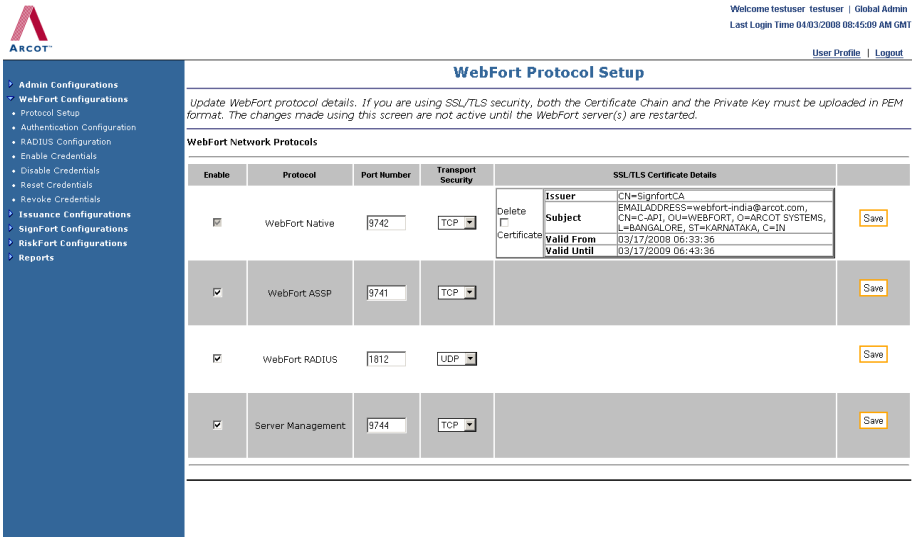
`<install_location>/arcot/conf/`

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

1. Under **WebFort Configurations** from the left-hand menu, select **Protocol Setup.**

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

Figure 4-4



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

   a. In the **Enable** column, ensure that the box corresponding to **WebFort Native** is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

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

a. Navigate to the following location:

`<install_location>/arcot/conf/`

b. Open the `adminserver.ini` file in an editor window.

c. In the `[arcot/admin/authconfig]` section, set the following parameters:

- `transport=TLS` (By default, this parameter is set to TCP.)
- `server.CACert=<absolute_path_of_Root_Certificate>`

d. Save the changes and close the file.

4. Restart WebFort Server as follows:

a. Navigate to the following directory:

`<install_location>/arcot/bin/`

b. Run the following command:

```
./webfortserver restart
```

5. Restart the application server.

Between RiskFort Server and Java SDKs

To enable TLS communication between RiskFort Server and Java SDKs, you must first configure the RiskFort protocols (Server Management, RiskFort Native, and Issuance) settings by using the Administration Console and then configure the applicable INI or properties files.

The INI file for **Server Management** is available at:

`<install_location>/arcot/conf/`

The properties files for **RiskFort Native** and **Issuance** are available at:

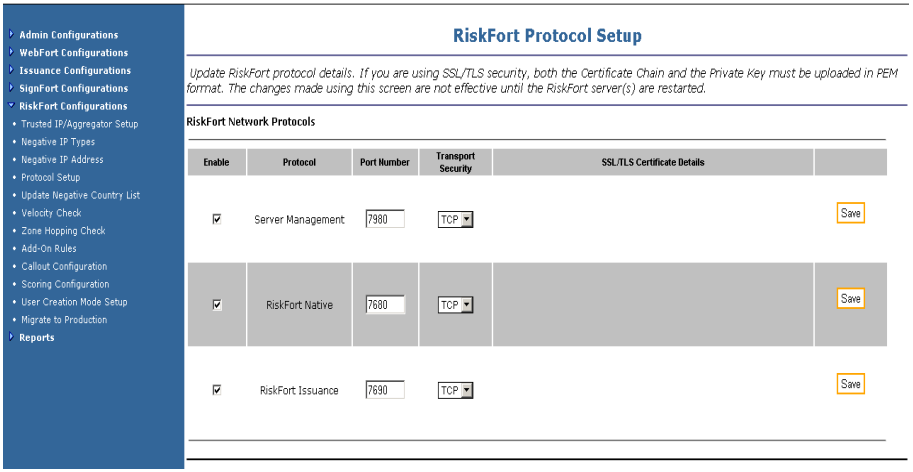
`<install_location>/arcot/sdk/java/properties/`

Perform the following tasks to enable TLS communication mode between RiskFort Server and Java SDKs:

1. Under **RiskFort Configurations** from the left-hand menu, select **Protocol Setup.**

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

Figure 4-5



2. Configure the **Server Management** protocol as follows:

   a. In the **Enable** column, ensure that the box corresponding to **Server Management** is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

   e. Navigate to the following location:

   `<install_location>/arcot/conf/`

   f. Open the **`arcotcommon.ini`** file in an editor window.

g. At the end of the file, add the following:

```
[arcot/aradmin/tlsconfig]

ServerCACert=
```

h. Set the following parameters:

- `ServerCACert=<absolute_path_of_Root_Certificate_in_PEM_FORMAT>`

  For example, you can specify `ServerCACert=<install_location>/certs/<ca_cert>.pem`.

  See "arcotcommon.ini" for more information on the configuration parameters.

i. Save the changes and close the file.

3. Configure the **RiskFort Native** protocol as follows:

   a. In the **Enable** column, ensure that the box corresponding to **RiskFort Native** is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

   e. Navigate to the following location:

   `<install_location>/arcot/sdk/java/properties/`

   f. Open the **`riskfort.properties`** file in an editor window.

   g. Set the following parameters:

- `TRANSPORT_TYPE=TLS` (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.properties" for more information on the configuration parameters.

h. Save the changes and close the file.

4. Configure the **Issuance** protocol as follows:

   a. In the **Enable** column, ensure that the box corresponding to **RiskFort Native** is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

   e. Navigate to the following location:

   `<`*`install_location`*`>/arcot/sdk/java/properties/`

   f. Open the **`riskfort_issuance.properties`** file in an editor window.

   g. Set the following parameters:

      - `TRANSPORT_TYPE=TLS` (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.

h. Save the changes and close the file.

5. Restart RiskFort Server as follows:

   a. Navigate to the following directory:

      `<install_location>/arcot/bin/`

   b. Run the following command:

      ```
      ./riskfortserver restart
      ```

6. Restart the application server.

Between RiskFort Server and Web Services

To enable TLS communication between RiskFort Server and Web Services, you must first configure the RiskFort protocols (**RiskFort Native** and **Issuance**) settings by using the Administration Console and then configure the applicable files on your application server that are available at:

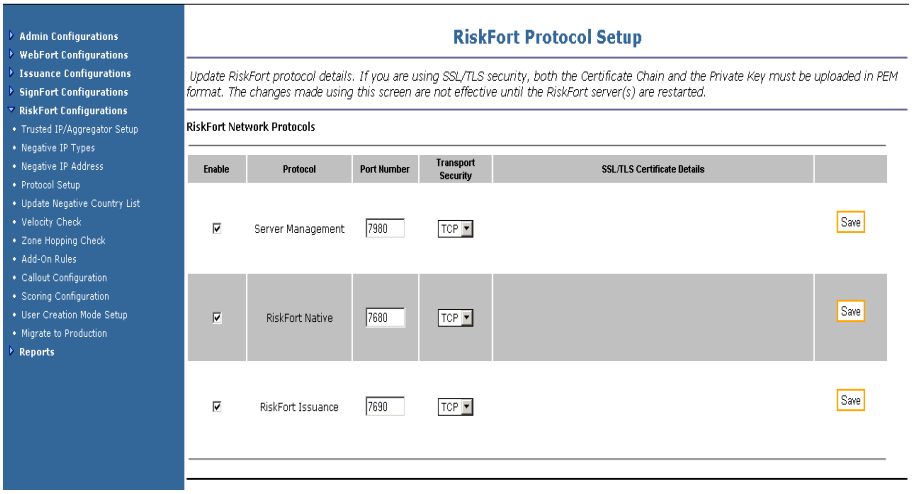
`<Application_Home>/WEB-INF/classes/properties/`

Perform the following tasks to enable TLS communication mode between RiskFort Server and Web Services:

1. Under **RiskFort Configurations** from the left-hand menu, select **Protocol Setup.**

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

Figure 4-6



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

   c. In the **Enable** column, ensure that the box corresponding to **RiskFort Native** is selected.

   d. In the **Transport Security** column, select **TLS** from the drop-down list.

   e. In the **SSL/TLS Certificate Details** column:

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

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

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

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

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

   g. Navigate to the following location of your application server:

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

   h. Open the **`riskfort.properties`** file in an editor window.

i. Set the following parameters:

- `TRANSPORT_TYPE=TLS` (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.properties" for more information on the configuration parameters.

j. Save the changes and close the file.

3. Configure the **Issuance** protocol as follows:

a. In the **Enable** column, ensure that the box corresponding to **Issuance** is selected.

b. In the **Transport Security** column, select **TLS** from the drop-down list.

c. In the **SSL/TLS Certificate Details** column:

I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

e. Navigate to the following location of your application server:

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

f. Open the **`riskfort_issuance.properties`** file in an editor window.

g. Set the following parameters:

- `TRANSPORT_TYPE=TLS` (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.

h. Save the changes and close the file.

4. Restart RiskFort Server as follows:

   a. Navigate to the following directory:

      <*install_location*>/arcot/bin/

   b. Run the following command:

      ```
      ./riskfortserver restart
      ```

5. Restart the application server.

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. To deploy the Sample Application:

1. Stop the application server services.
2. Deploy the `riskfort-1.7-sample-application.war` file *from* the following location:

   <*install_location*>/arcot/samples/java/

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

3. Start the application server services.

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

Configuring Sample Application for Communication with RiskFort Server

The `riskfort.properties` file provides the parameters for the Java SDK and Sample Application to read RiskFort Server information. Therefore, after deploying 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-1.7-sample-application.war`.

To configure the `riskfort.properties` file:

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

   In case of Apache Tomcat this file is available at:

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

   Here, *AppHome*`/riskfort-1.7-sample-application` represents the directory path where RiskFort application WAR files are deployed.

2. Open the `riskfort.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.properties" for more information on configuration parameters.

3. (**Optional:** Perform this step only if you configured TLS-based communication in "(Optional) Configuring TLS Communication Mode")

   Set the following parameters:

- `TRANSPORT_TYPE=TLS` (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`

4. Save the changes and close the file.
5. Restart the application server for the changes to take effect.

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:

- **Creating User**
- **Performing Risk Evaluation and Post Evaluation**
- **Editing the Default Profile and Performing Risk Evaluation**

Creating User

To create a user:

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

   `http://<host>:<port>/riskfort-1.7-sample-application/index.jsp`

   The RiskFort Sample Application page appears.
2. Click **User Creation** to open the Create User page.
3. Enter a unique user name in the **User Name** field and click **Create User.**

   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

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-1.7-sample-application/index.jsp`

2. Click **Risk Evaluation** to open the Risk Evaluation on my default Profile page.
3. On the page, specify the name of the user (who you want to evaluate) in the **Enter the User Name** field.
4. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score and the associated Risk Advice for the specified user.

5. Click **Next Step** to open the Post Evaluation page and perform post-evaluation on the specified user profile.
6. Specify the result of secondary authentication by selecting the appropriate option from the **Result of Secondary Authentication** list.
7. Click **Post Evaluate** to complete the post evaluation process and display the result of the same.

Editing the Default Profile and Performing Risk Evaluation

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

1. Ensure that Sample Application is open (in a Web browser window.)
2. Click **Risk Evaluation** to open the Risk Evaluation on my default Profile page.
3. On the page, specify the name of the user (whose profile you want to edit) in the **Enter the User Name** field.
4. Click **Edit My Profile** to open the Edit My Profile page.
5. On the page, the following fields are pre-populated:

   - **IP Address of My Machine**
   - **Device ID of My Machine**

   If you want to change any or both these values, specify the new value.

6. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score and the associated Risk Advice for the specified user.

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 the post evaluation process and display the result of the same.

Chapter 5

Deploying RiskFort on a Distributed System

Use the **Arcot RiskFort 1.7 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 "Running Database Scripts" and "Verifying the Database Setup" for more information.

3. Deploy Administration Console on the application server and verify the deployment.

   See "Deploying Administration Console" and "Verifying the Administration Console Deployment" for more information.

4. Log in to Administration Console with the Master Administrator credentials to initialize RiskFort and then create a Global Administrator.

   See "Logging in to Administration Console" and "Creating a Global Administrator" for more information.

5. To ensure secure communication between RiskFort components, you can configure them to support TLS (Transport Layer Security) transport mode. This is an optional step.

   See "(Optional) Configuring TLS Communication" for more information to do so on the first system and "(Optional) Configuring TLS Communication" for more information to do so on the subsequent system.

6. Install the Java SDKs on one or more systems.

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

7. Perform post-installation tasks on the system where Java SDKs and Web Services are installed.

   See "(Optional) Configuring TLS Communication" for more information.

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

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

Important Notes Related to Installation

You must keep the following points in mind while installing RiskFort:

- You must ensure that the `<install_location>` *must not contain* any special characters (such as ~ ! @ # $ % ^ & * ( ) _ + = { } [ ] ' ").
- RiskFort 1.7 does not support upgrade from a previous version (1.6.1 or earlier). Also, you can not install RiskFort 1.7 over a previously installed version.
- Currently, you can not modify or repair RiskFort components by using the installer. You *must* uninstall the component and then re-install it.
- The installation directory name that you specify *must not* contain any spaces. If there are spaces in the installation directory name, some of the RiskFort scripts might not function as intended.
- During Custom installation:
  - If you enter the number of main features (1, 5, or 8), then all the sub-features of the main feature will be implicitly selected.
  - If you enter the number of a sub-feature, then only the selected sub-feature will be installed.
  - If you enter the number of a main feature and any of its sub-feature, then the selected sub-feature will not be installed.

Installing on the First System

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. You use the *Custom installation* option to install only the selected components from the package.

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"**.

> **NOTE:** Any time during the installation, you can type `quit` and press **Enter** to exit the installation.

Perform the following tasks to install RiskFort components:

1. Log in and navigate to the location where `Arcot-RiskFort-1.7-Linux.tar.gz` is located.
2. Uncompress and untar the installer.
3. Navigate to the directory where you untarred the installer.
4. Run the installer as follows:

   ```
   prompt> sh Arcot-RiskFort-1.7-Linux-Installer.bin
   ```

   If you are executing the installer with `root` login, then a warning message appears. Enter **Y** to continue, or enter **N** to quit the installation.

   If you exit the installer screen, then you must run the installer again.

5. Press **Enter** to continue.

   The Welcome screen appears.

6. Press **Enter** to continue with the installation.

   The License Agreement for RiskFort appears.

7. On the License Agreement screen:

   a. Read the text carefully and press **Enter** to display the next screen of the license text. You might have to press **Enter** multiple times, until the entire text for License Agreement is displayed.

      At the end of the license agreement, you will be prompted for acceptance of the terms of license agreement.

b. Enter **y** to accept the acceptance of License Agreement and to continue with the installation.

NOTE: If you press **n**, then a warning message will be displayed and the installation will be aborted.

The Choose Installation Location screen appears.

8. As directed on the screen, you can *either*:

- Enter the absolute path of the directory where you want to install RiskFort and press **Enter** to continue.

NOTE: The installation directory name that you specify *must not* contain any spaces. Else, some RiskFort scripts and tools might not function as intended.

- Press **Enter** to accept the default directory displayed by the installer.

The installer displays the installation options supported by RiskFort.

9. If the computer where you are currently performing the installation already has an existing Arcot product installed, then the installer displays the following options:

- **1** - Enter a new location.
- **2** - Continue to install in the directory selected in **Step 8.**
- **3** - Use the location at which the existing Arcot product is installed.

10. Select the required option and press **Enter** to continue with the installation.

NOTE: If you selected option 1 or 2, then a new directory `arcot` will be created in the specified location.

The Choose Install Type of Installation screen appears. This screen displays the installation types (Complete and Custom) supported by RiskFort.

11. Type **2** and press **Enter** to accept the **Custom** installation option and to continue with the installation.

The Choose Product Features screen appears. This screen enables you to select the specific components that you wish to install on the system.

12. Specify a comma-separated list of numbers representing the RiskFort components you would like to install and press **Enter** to continue.

NOTE: To install the Sample Application *only*, you must ensure that you select only the **Risk Evaluation SDK** *and* the **Issuance SDK** options and proceed with the installation.

The following table describes all components that are installed by the RiskFort installer.

Table 5-1 Components Installed by RiskFort

Components	Description
RiskFort Evaluation	This option provides the risk evaluation service. This package comprises the following sub-components: • RiskFort Server - Provides transaction and session risk evaluation. • RiskFort SDK - Provides the Java programming interface for risk evaluation with RiskFort Server. • RiskFort Web Services - Provides the Web-based programming interface for risk evaluation with RiskFort Server. Refer to the Chapter 6, "Configuring RiskFort SDKs and Web Services"for more information on configuring these components.
Issuance	This option provides programming interfaces for creation and management of users. This package comprises the following sub-components: • Issuance SDK - Provides the Java programming interface for creation and management of users. • Issuance Web Services - Provides the We-based programming interface for creation and management of users. Refer to the Chapter 6, "Configuring RiskFort SDKs and Web Services"for more information on configuring these components.
Administration Console	This option provides Web-based interface for Server configuration and administration of credentials and users. **IMPORTANT:** If you selected the **Administration Console** component on this screen, then you *must* perform **Basic** installation of WebFort. Refer to the section, "WebFort Basic Installation" for more information.

NOTE: If RiskFort Evaluation was not selected for installation on this screen, then screens in Step 13 through Step 18 will not appear.

The ODBC Home Configuration screen appears. This screen prompts you to specify the path to the ODBC Driver.

13. Enter the absolute search path (for example, `/opt`) where the ODBC driver for the database is available, and press **Enter** to continue.

    The installer checks for the ODBC drivers present in the specified location. If multiple versions are found, then the installer displays all versions and prompts you to select one. If no ODBC driver is found in the specified location, then you are prompted for another location.

    The Oracle Home Configuration screen appears. This screen prompts you to specify the Oracle Client path.

14. Enter the absolute search path where Oracle Client is available, and press **Enter** to continue.

    The installer checks for Oracle Client in the specified location. If multiple entries are found, then the installer displays all of them and prompts you to select one. If no Oracle Client is found in the specified location, then you are prompted for another location.

    The Java Home Configuration screen appears.

15. Enter the absolute search path for JAVA HOME and press **Enter** to continue.

    The installer checks for `JAVA HOME` in the specified location. If multiple versions are found, then the installer displays all and prompts you to select one. If no `JAVA HOME` is found in the specified location, then you are prompted for another location.

    The Primary Database Access Configuration screen appears.

16. On the Primary Database Access Configuration screen:

    a. Specify the name of the DSN, when prompted, and press **Enter.**

       The installer checks for the availability of the specified DSN. If this DSN is already present, then appropriate messages are displayed.

    b. Specify the appropriate choice (**1**, **2**, or **3**) and press **Enter** to continue.

       The installer now prompts you for more information related to the specified DSN.

c. Specify the information listed in the following table.

Table 5-2 Primary DSN Parameters

Parameter	Description
TNS Service Name	Transparent Network Substrate (TNS) is used by Oracle databases and specifies the name by which an Oracle database instance is known on a network. In other words, TNS Name resolves to the protocol, IP, port, and SID of an oracle database. The name can be found in the `tnsnames.ora` file on the local system.
User Name	The database user name for RiskFort to access the database. This name is specified by the database administrator. **NOTE:** The User Name 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.
SID	The Oracle System Identifier (SID) that refers to the instance of the Oracle database running on the server.
Port No	The port at which the Database listens to the incoming requests.
Host Name	The host name or IP address of the RiskFort datastore. **Syntax**: *<server_name>* **Example**: `demodatabase`

d. Enter **Y** to test connectivity to the specified database, or **N** to skip this test.

The Backup Database Access Configuration screen appears.

17. On the Backup Database Access Configuration screen:

- Type **N** to skip the configuration of the secondary DSN, when prompted, and press **Enter** to continue to the next screen.
- Type **Y** to configure the secondary DSN, when prompted, and press **Enter** to continue.

  See the sub-steps of **Step 16** for more information on the tasks to be performed.

The WebFort Connectivity screen appears.

18. Specify the Host Name and the Port number of WebFort Server and press **Enter** to continue. This information is required by Administration Console to connect to WebFort and authenticate the RiskFort administrators.

    The Pre-Installation Summary screen appears. This screen lists the product details, installation directory, type of installation, components that are to be installed, and disk space-related information.

19. Review the product details displayed carefully and press **Enter** to proceed with the installation. If you would like to change a configuration on any of the previous screens, type **back** until you reach the screen, make the required changes, and press **Enter** to proceed to the next screen.

    The Installing screen appears. This might take several minutes, because the installer now:

    - Puts all the components and their related binaries in the installation directory.
    - Stores database settings in the **arcotcommon.ini** file and the password in the `securestore.enc` file.
    - Writes to the required INI files.
    - Sets the environment variables such as, `JNI_LIBRARY_PATH` for Issuance and Administration Console and `ODBC_HOME`, `ODBCINI`, `ORACLE_HOME`, and `ORACLE_LIB_PATH` in the `arctenv` file.
    - Creates or overwrites, as specified in a previous screen, the Primary DSN and Backup DSN (if selected and configured) using the selected ODBC driver in the `odbc.ini` file.

    After the preceding tasks are completed successfully, the Installation Complete screen appears.

20. Press **Enter** to exit the installer.

    You might have to wait for a few minutes (for the installer to clean up temporary files) until the prompt re-appears.

21. Check the installation log file, which is available in the `<install_location>/arcot/` directory.

22. Perform **WebFort Basic Installation**:

    a. Navigate to the directory where the `Arcot-WebFort-5.4.1-Linux.tar.gz` file is located.

    b. Gunzip and untar the file, and then run the installation wizard, as follows:

    ```
    prompt>sh Arcot-WebFort-5.4.1-Linux-Installer.bin
    ```

c. Follow the instructions on the following screens to install. On the Type of Installation screen, you must enter **2** to specify the **Basic** option.

   See the *Arcot WebFort Installation and Deployment Guide* for detailed instructions to perform WebFort Basic 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 in the following directory:

`<install_location>/arcot/logs/`

If for some reason, the installation failed, then the error log is available in the `/tmp` directory.

WebFort Basic Installation

The Administration Console is a common component included in many Arcot products. It uses WebFort Server to authenticate users when they log in. As a result, WebFort is a required component for other Arcot products, including RiskFort.

However, WebFort Basic is not packaged as a part of RiskFort. To configure Administration Console to access WebFort, it is highly recommended that you perform **Basic** installation of WebFort *after* completing the installation of RiskFort. The Basic deployment installs only WebFort Server.

NOTE: Refer to the *Arcot WebFort Installation and Deployment Guide* for detailed steps for performing WebFort **Basic** installation.

While performing WebFort **Basic** installation, if the corresponding RiskFort DSN configuration has already been completed, then you will not be prompted for the DSN-related information. However, if the DSN has not already been configured, then you will need to specify this information in the additional screens that appear.

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. Running Database Scripts
2. Verifying the Database Setup
3. Verifying the Installation
4. Deploying Administration Console
5. Verifying the Administration Console Deployment
6. Logging in to Administration Console
7. Creating a Global Administrator
8. (Optional) Configuring TLS Communication
9. Deploying Sample Application
10. Configuring Sample Application for Communication with RiskFort Server
11. Using Sample Application

Running Database Scripts

> **NOTE:** 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" section.

> **NOTE:** 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" 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/dbscripts/oracle/`

2. Run the scripts *in the following order*:

- `arcot-db-initial-config-common-1.0.sql`
- `arcot-db-config-for-webfort-5.4.1.sql`
- `arcot-db-config-for-riskfort-1.7.sql`

Verifying the Database Setup

After the database has been set up, you must verify whether the database was set up correctly. To do so, perform the following tasks:

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

```
SELECT SERVERNAME, VERSION FROM ARSERVERS;
```

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

```
SERVERNAME                VERSION
------------------------  ----------------
WebFort                     5.4.1
RiskFort                    1.7
Admin Console               5.4.1
WebFort Issuance            5.4.1
```

3. Log out of the database console.

Verifying the Installation

After you have run the database scripts mentioned in the **"Running Database Scripts"** section to create the required tables, you must verify whether RiskFort was installed correctly. Perform the following tasks to do so:

1. **Starting the RiskFort Server**
2. **Verifying the Log Files**

Starting the RiskFort Server

Perform the following steps to start the RiskFort Server:

1. Navigate to the following directory:

<*install_location*>/arcot/bin/

2. Run the following commands:

```
./webfortserver start
./riskfortserver start
```

After starting the server, you must check if the server started successfully. To do so:

1. Navigate to the following directory:

   `<install_location>/arcot/logs/`

2. Open the `arcotriskfort.log` file by using any editor.
3. Locate the following line in the file:

```
Arcot RiskFort Service READY
```

Stopping the RiskFort Server

If at any time, you want to stop the RiskFort or WebFort Server, then perform the following steps to do so:

Perform the following steps to start the RiskFort and WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following commands:

   - `./riskfortserver stop [server_ip_address] [server_management_port_number]`

     The default value for *server_management_port_number* is `7980`. This is a configurable value.

   - `./webfortserver stop [server_ip_address] [server_management_port_number]`

     The default value for *server_management_port_number* is `9743`. This is a configurable value.

Verifying the Log Files

The two log files that you need to verify if the RiskFort and WebFort servers started correctly are:

- `arcotriskfort.log`
- `arcotwebfort.log`

Perform the following steps to verify if the servers started correctly:

1. Navigate to the following location:

   `<install_location>/arcot/logs/`

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

   - `STARTING Arcot RiskFort 1.7.0_1`

     This is the first line in the file.

   - `Arcot RiskFort Service READY`

     This is the last line in the file.

3. Open the `arcotwebfort.log` file in any editor and locate the following lines:

   - `STARTING Arcot WebFort 5.4.1_1`

     This is the first line in the file.

   - `Arcot WebFort Authentication Service READY`

     This is the last line in the file.

     NOTE: You might also want to make sure that the log files do not contain any FATAL messages.

Deploying Administration Console

The Administration Console is a browser-based interface to RiskFort that enables you to customize the server configurations, if required.

> **NOTE:** Arcot strongly recommends that you configure the Administration Console *after* you have completed the **Basic** WebFort installation. Refer to the *Arcot WebFort Installation and Deployment Guide* for detailed steps for performing WebFort Basic installation.

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

`<install_location>/arcot/java/app/admin/`

To deploy the WAR file on your application server:

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

   The deployment directory and procedure will depend on the application server that you are using. Refer to your Application server documentation for detailed instructions.

   For example, in case of Apache Tomcat, you must deploy the `arcotadmin.war` file in the following location:

   `<APP_SERVER_HOME>/webapps/`

2. Navigate to the `<install_location>/arcot/sbin/` directory.
3. Run the following command to set the required environment variables:

   ```
   . ./arctenv
   ```

4. Start the application server.

Verifying the Administration Console Deployment

The `arcotadmin.log` file is used for logging the Administration Console information. This file is available in the `<APP_SERVER_HOME>` of your application server.

After you deploy the Administration Console successfully, navigate to the `arcotadmin.log` file, open it any editor, and locate the following lines:

- `Title: Arcot Admin Console, Vendor: Arcot Systems Inc., Version No:5.4.1`
- `Servlet 'cygnetadmin' configured successfully`

These lines indicate that your Administration Console was deployed successfully.

Changing the Default Log File Location

By default, the log files for Administration Console are generated in the default log directory of your application server. However, you might want to specify a different directory to store the log files for Administration Console. In this case, perform the following steps:

1. Navigate to the `<APP_SERVER_HOME>` directory.
2. Navigate to the subdirectory where the `log4j.properties` file is located.
3. Open the `log4j.properties` file in any editor window.

4. Locate the `log4j.appender.debuglog.File` property and specify the absolute file path to the `arcotadmin.log` file as its value.

   For example:

   `log4j.appender.debuglog.File=<install_location>/arcot/logs/arcotadmin.log`

5. Restart application server for the change to take effect.

Logging in to Administration Console

> **NOTE:** You *must* start the RiskFort and WebFort Servers before attempting to log in into Administration Console application.

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

To log in to the Administration Console:

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

   `http://<host>:<port>/arcotadmin/adminlogin.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:** Master_Admin
   - **Password:** master1234

     > **NOTE:** 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.

Creating a Global Administrator

When you install and configure RiskFort, the *Master Administrator* account is created by default. However, this account can only perform restricted activities, such as initializing the system and creating the next level of administrators, called Global Administrator. For any advanced configurations, you must now create at least one Global Administrator account.

Global Administrators are responsible for configuring the global settings and setting up the communication protocol. They can also create next level of administrators and manage their credentials.

> **NOTE:** Refer to *Arcot RiskFort Administration Guide* for more information on Global administrator privileges.

To create a Global Administrator account:

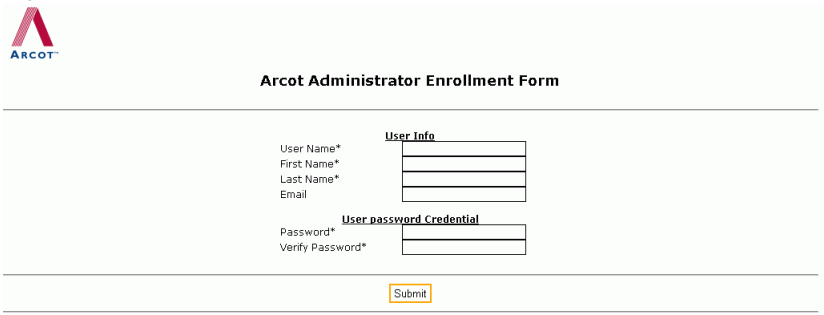
1. Access the Administration Console by using the following URL:

   `http://<host>:<port>/arcotadmin/adminlogin.htm`

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

   The Arcot Administrator Enrollment Form page, as shown in following figure, appears.

Figure 5-1



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

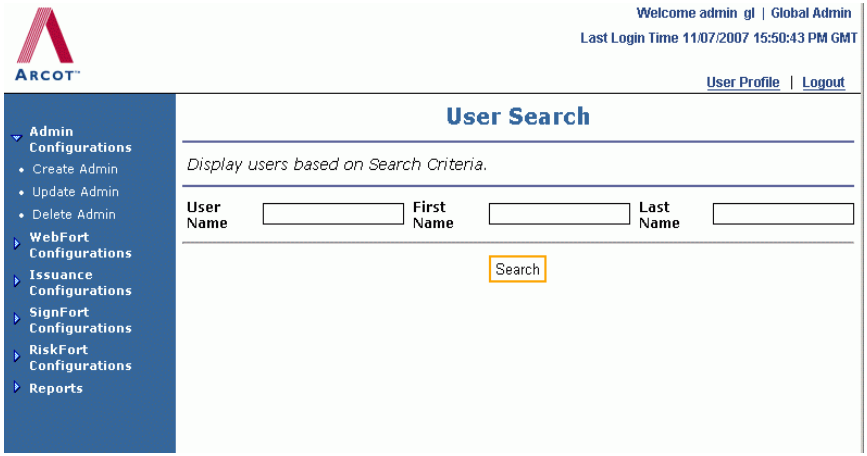
   > **NOTE:** Fields marked with * are mandatory fields. The field **User Name** is not case sensitive.

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

4. Log in as Master Administrator again.
5. Under **Admin Configurations**, select the **Create Admin** option.

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

Figure 5-2

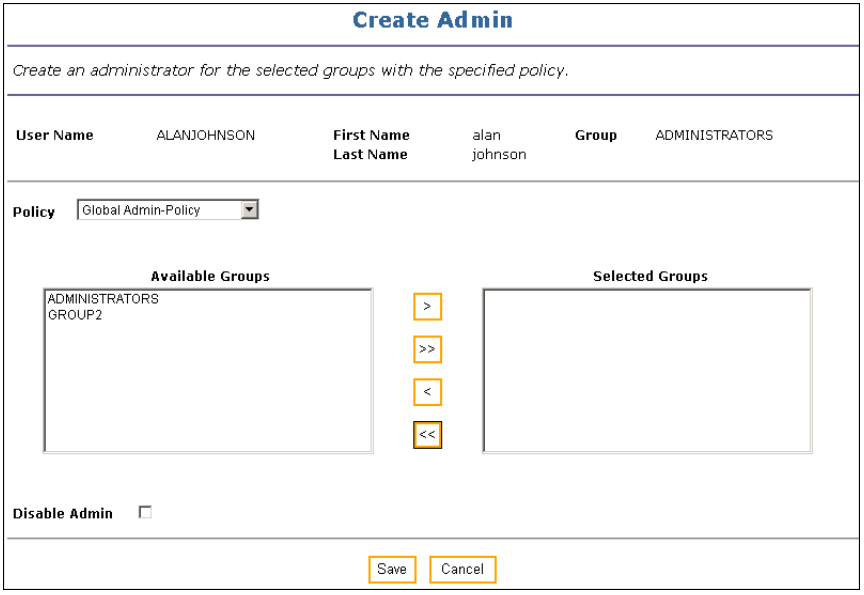


6. Provide complete or partial details of the user and click the **Search** button.

   A list of enrolled users matching the search criteria and who are not administrators is displayed.
7. Click the **User Name** link for the user you want to promote as an administrator.

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

Figure 5-3



8. To specify the level of the administrator, you must select the policy to be associated. Select the **Global Admin-Policy** option from the **Policy** drop-down list.

9. Select the group from the **Available Groups** list and click the > button to add the group to the **Selected Groups** list.

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

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

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

    The "Admin created successfully" message appears.

(Optional) Configuring TLS Communication

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 WebFort Server and between SDKs and RiskFort Server, you can configure RiskFort Native and Server Management protocols to support TLS (Transport Layer Security), which ensures securer communication between applications across insecure media and reduces the chances of TCP attacks.

This section discusses the steps to configure TLS-based communication between WebFort Server and Administration Console.

Between WebFort Server and Administration Console

By default, Administration Console uses Transmission Control Protocol (TCP) to communicate with WebFort Server. (See **"WebFort Basic Installation"** for more information.)

To enable TLS communication between WebFort Server and Java SDKs, you must first configure the WebFort Native protocol settings by using the Administration Console and then configure the **`adminserver.ini`** file, which is available at:

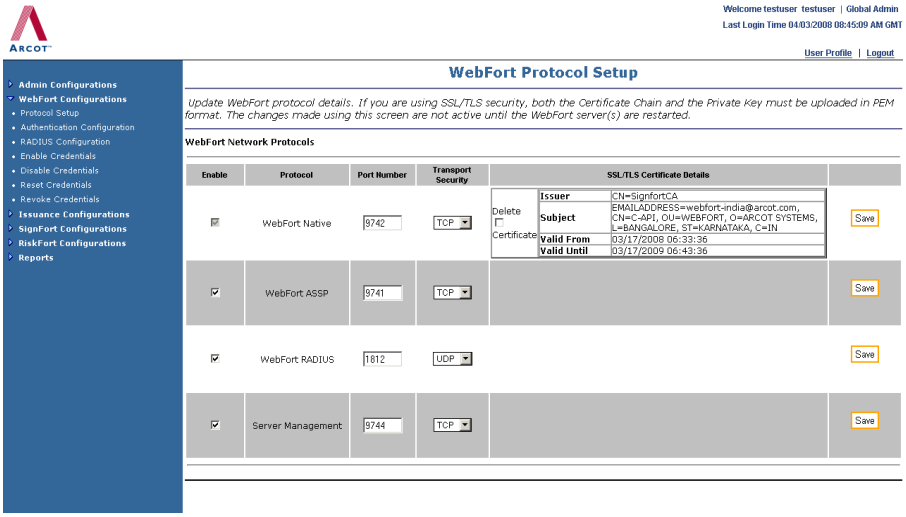
`<install_location>/arcot/conf/`

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

1. Under **WebFort Configurations** from the left-hand menu, select **Protocol Setup.**

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

Figure 5-4



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

   d. In the **Enable** column, ensure that the box corresponding to **WebFort Native** is selected.

   e. In the **Transport Security** column, select **TLS** from the drop-down list.

   f. In the **SSL/TLS Certificate Details** column:

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

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

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

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

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

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

a. Navigate to the following location:

`<install_location>/arcot/conf/`

b. Open the `adminserver.ini` file in an editor window.

c. In the `[arcot/admin/authconfig]` section, set the following parameters:

- `transport=TLS` (By default, this parameter is set to TCP.)
- `server.CACert=<absolute_path_of_Root_Certificate>`

d. Save the changes and close the file.

4. Restart WebFort Server as follows:

a. Navigate to the following directory:

`<install_location>/arcot/bin/`

b. Run the following command:

```
./webfortserver start
```

5. Restart the application server.

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: Before you proceed with the steps to deploy Sample Application, you must ensure that the system where you are deploying the application must have `ARCOT_HOME` configured and `regfort.ini` file available.

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 **Risk Evaluation SDK** *and* the **Issuance SDK** options and proceed with the installation.

To deploy the Sample Application:

1. Stop the application server services.

2. Deploy the `riskfort-1.7-sample-application.war` file *from* the following location:

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

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

3. Start the application server services.

Configuring Sample Application for Communication with RiskFort Server

The `riskfort.properties` file provides the parameters for the Java SDK and Sample Application to read RiskFort Server information. Therefore, after deploying 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-1.7-sample-application.war`.

To configure the `riskfort.properties` file:

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

   In case of Apache Tomcat this file is available at:

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

   Here, *AppHome/*`riskfort-1.7-sample-application` represents the directory path where RiskFort application WAR files are deployed.

2. Open the `riskfort.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.properties" for more information on configuration parameters.

3. (**Optional:** Perform this step only if you configured TLS-based communication in "(Optional) Configuring TLS Communication")

   Set the following parameters:

   - `TRANSPORT_TYPE=TLS` (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`

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

See "riskfort.properties" for more information on configuration parameters of this file.

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:

- Creating User
- Performing Risk Evaluation and Post Evaluation
- Editing the Default Profile and Performing Risk Evaluation

Creating User

To create a user:

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

   `http://<host>:<port>/riskfort-1.7-sample-application/index.jsp`

   The RiskFort Sample Application page appears.

2. Click **User Creation** to open the Create User page.

3. Enter a unique user name in the **User Name** field and click **Create User.**

   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

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-1.7-sample-application/index.jsp`

2. Click **Risk Evaluation** to open the Risk Evaluation on my default Profile page.

3. On the page, specify the name of the user (who you want to evaluate) in the **Enter the User Name** field.

4. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score and the associated Risk Advice for the specified user.

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

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

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

Editing the Default Profile and Performing Risk Evaluation

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

1. Ensure that Sample Application is open (in a Web browser window.)

2. Click **Risk Evaluation** to open the Risk Evaluation on my default Profile page.

3. On the page, specify the name of the user (whose profile you want to edit) in the **Enter the User Name** field.

4. Click **Edit My Profile** to open the Edit My Profile page.

5. On the page, the following fields are pre-populated:

- **IP Address of My Machine**
- **Device ID of My Machine**

If you want to change any or both these values, specify the new value.

6. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score and the associated Risk Advice for the specified user.

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 the post evaluation process and display the result of the same.

Installing on the Second System

After installing RiskFort Server and Administration Console, you must now install the other 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"**.

Perform the following steps to install RiskFort components:

1. Copy the installer file `Arcot-RiskFort-1.7-Linux.tar.gz` on the target (second) system.
2. Run the installer as follows:

   ```
   prompt> sh Arcot-RiskFort-1.7-Linux-Installer.bin
   ```

3. Follow the installer instructions from **Step 5** until you reach the **Choose Install Set** screen.
4. Select the components you wish to install.

   Typically, you will be installing the Java SDKs or the Web Services for Risk Evaluation and Issuance.

5. After you have selected all the components, follow the from **Step 13** through **Step 20** to complete the installation.

   NOTE: If RiskFort Evaluation was not selected for installation on this screen, then screens in **Step 13** through **Step 18** will not appear.

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. **(Optional) Configuring TLS Communication**
2. **Deploying Sample Application**
3. **Configuring Sample Application for Communication with RiskFort Server**
4. **Using Sample Application**

(Optional) Configuring TLS Communication

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 RiskFort components, you must configure them to TLS (Transport Layer Security) transport mode.

This section discusses the steps to configure TLS-based communication:

- **Between RiskFort Server and Java SDKs**
- **Between RiskFort Server and Web Services**

Between RiskFort Server and Java SDKs

To enable TLS communication between RiskFort Server and Java SDKs, you must first configure the RiskFort protocols (Server Management, RiskFort Native, and Issuance) settings by using the Administration Console and then configure the applicable INI or properties files.

The INI file for **Server Management** is available at:

`<install_location>/arcot/conf/`

The properties files for **RiskFort Native** and **Issuance** are available at:

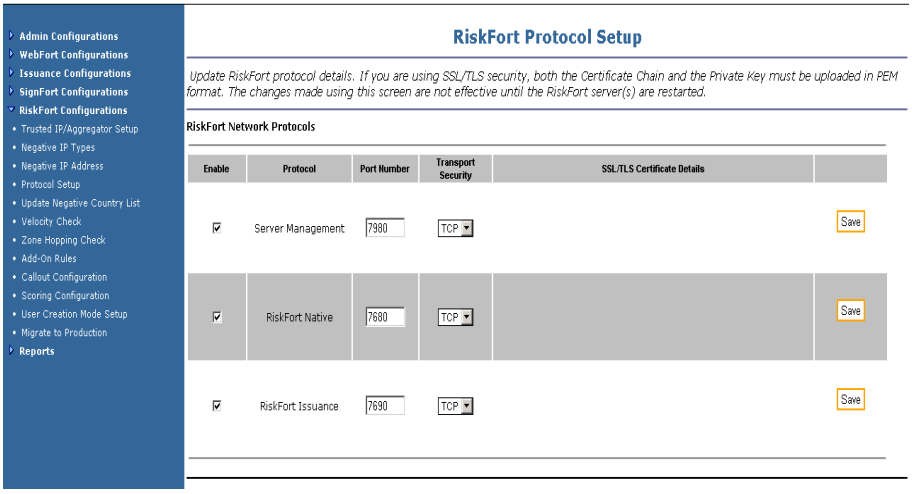
`<install_location>/arcot/sdk/java/properties/`

Perform the following tasks to enable TLS communication mode between RiskFort Server and Java SDKs:

1. Under **RiskFort Configurations** from the left-hand menu, select **Protocol Setup.**

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

Figure 5-5



2. Configure the **Server Management** protocol as follows:

   a. In the **Enable** column, ensure that the box corresponding to **Server Management** is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

e. Navigate to the following location:

`<install_location>/arcot/conf/`

f. Open the **`arcotcommon.ini`** file in an editor window.

g. At the end of the file, add the following:

```
[arcot/aradmin/tlsconfig]

ServerCACert=
```

h. Set the following parameters:

- `ServerCACert=<absolute_path_of_Root_Certificate_in_PEM_FORMAT>`

  For example, you can specify `ServerCACert=<install_location>/certs/<ca_cert>.pem`.

  See "arcotcommon.ini" for more information on the configuration parameters.

i. Save the changes and close the file.

3. Configure the **RiskFort Native** protocol as follows:

   a. In the **Enable** column, ensure that the box corresponding to **RiskFort Native** is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

e. Navigate to the following location:

`<install_location>/arcot/sdk/java/properties/`

f. Open the **`riskfort.properties`** file in an editor window.

g. Set the following parameters:

- `TRANSPORT_TYPE=TLS` (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.properties" for more information on the configuration parameters.

h. Save the changes and close the file.

4. Configure the **Issuance** protocol as follows:

a. In the **Enable** column, ensure that the box corresponding to **RiskFort Native** is selected.

b. In the **Transport Security** column, select **TLS** from the drop-down list.

c. In the **SSL/TLS Certificate Details** column:

I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

e. Navigate to the following location:

`<install_location>/arcot/sdk/java/properties/`

f. Open the **`riskfort_issuance.properties`** file in an editor window.

g. Set the following parameters:

- `TRANSPORT_TYPE=TLS` (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.

h. Save the changes and close the file.

5. Restart RiskFort Server as follows:

   a. Navigate to the following directory:

   `<install_location>/arcot/bin/`

   b. Run the following command:

   ```
   ./riskfortserver restart
   ```

6. Restart the application server.

Between RiskFort Server and Web Services

To enable TLS communication between RiskFort Server and Web Services, you must first configure the RiskFort protocols (**RiskFort Native** and **Issuance**) settings by using the Administration Console and then configure the applicable files on your application server that are available at:

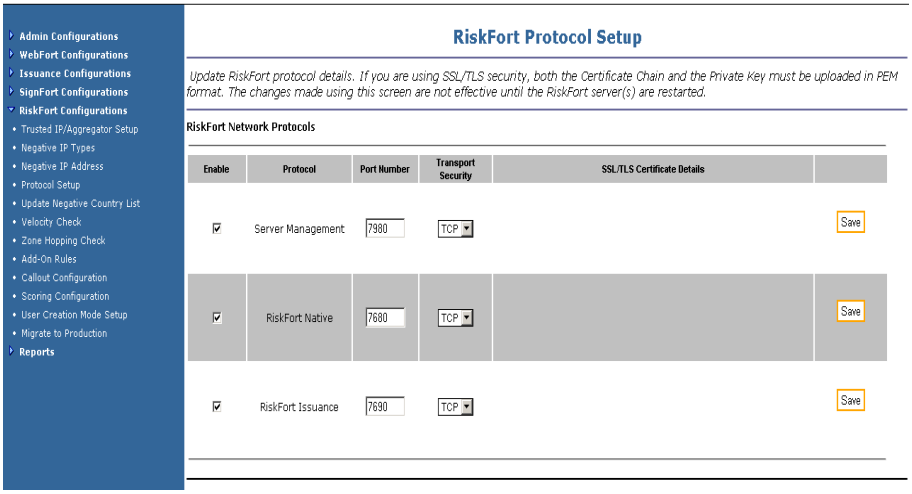
`<Application_Home>/WEB-INF/classes/properties/`

Perform the following tasks to enable TLS communication mode between RiskFort Server and Web Services:

1. Under **RiskFort Configurations** from the left-hand menu, select **Protocol Setup.**

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

Figure 5-6



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

   c. In the **Enable** column, ensure that the box corresponding to **RiskFort Native** is selected.

   d. In the **Transport Security** column, select **TLS** from the drop-down list.

   e. In the **SSL/TLS Certificate Details** column:

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

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

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

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

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

   g. Navigate to the following location of your application server:

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

   h. Open the **`riskfort.properties`** file in an editor window.

i. Set the following parameters:

- `TRANSPORT_TYPE=TLS` (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.properties" for more information on the configuration parameters.

j. Save the changes and close the file.

3. Configure the **Issuance** protocol as follows:

   a. In the **Enable** column, ensure that the box corresponding to **Issuance** is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the 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.

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

   e. Navigate to the following location of your application server:

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

   f. Open the **`riskfort_issuance.properties`** file in an editor window.

   g. Set the following parameters:

   - `TRANSPORT_TYPE=TLS` (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.

h. Save the changes and close the file.

4. Restart RiskFort Server as follows:

   a. Navigate to the following directory:

      <*install_location*>/arcot/bin/

   b. Run the following command:

      ```
      ./riskfortserver restart
      ```

5. Restart the application server.

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.

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

  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 **Risk Evaluation SDK** *and* the **Issuance SDK** options and proceed with the installation.

To deploy the Sample Application:

1. Stop the application server services.
2. Deploy the `riskfort-1.7-sample-application.war` file from the following location:

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

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

3. Start the application server services.

Configuring Sample Application for Communication with RiskFort Server

The `riskfort.properties` file provides the parameters for the Java SDK and Sample Application to read RiskFort Server information. Therefore, after deploying 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-1.7-sample-application.war`.

To configure the `riskfort.properties` file:

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

   In case of Apache Tomcat this file is available at:

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

   Here, `AppHome/riskfort-1.7-sample-application` represents the directory path where RiskFort application WAR files are deployed.

2. Open the `riskfort.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.properties"** for more information on configuration parameters.

3. (**Optional:** Perform this step only if you configured TLS-based communication in "(Optional) Configuring TLS Communication")

   Set the following parameters:

   - `TRANSPORT_TYPE=TLS` (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`

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:

- Creating Users
- Performing Risk Evaluation and Post Evaluation
- Editing the Default Profile and Performing Risk Evaluation

Creating Users

To create a user:

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

   `http://<host>:<port>/riskfort-1.7-sample-application/index.jsp`

   The RiskFort Sample Application page appears.

2. Click **User Creation** to open the Create User page.
3. Enter a unique user name in the **User Name** field and click **Create User.**

   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

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-1.7-sample-application/index.jsp`

2. Click **Risk Evaluation** to open the Risk Evaluation on my default Profile page.
3. On the page, specify the name of the user (who you want to evaluate) in the **Enter the User Name** field.
4. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score and the associated Risk Advice for the specified user.

5. Click **Next Step** to open the Post Evaluation page and perform post-evaluation on the specified user profile.
6. Specify the result of secondary authentication by selecting the appropriate option from the **Result of Secondary Authentication** list.
7. Click **Post Evaluate** to complete the post evaluation process and display the result of the same.

Editing the Default Profile and Performing Risk Evaluation

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

1. Ensure that Sample Application is open (in a Web browser window.)
2. Click **Risk Evaluation** to open the Risk Evaluation on my default Profile page.
3. On the page, specify the name of the user (whose profile you want to edit) in the **Enter the User Name** field.
4. Click **Edit My Profile** to open the Edit My Profile page.
5. On the page, the following fields are pre-populated:
   - **IP Address of My Machine**
   - **Device ID of My Machine**

   If you want to change any or both these values, specify the new value.

6. Click **Evaluate Risk** to open the Risk Evaluation Results page.

   This page displays the Risk Score and the associated Risk Advice for the specified user.

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 the post evaluation process and display the result of the same.

   NOTE: You must now configure RiskFort SDKs (and Web services), as discussed in **Chapter 6, "Configuring RiskFort SDKs and Web Services," on page 105**.

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:

Understanding RiskFort APIs

RiskFort is shipped with a set of Java APIs in the form of Java SDK (`arcot_riskfort_sdk.jar`), which is available in the following location:

`<install_location>/arcot/sdk/java/lib/arcot/arcot_riskfort_sdk.jar`

The APIs shipped with RiskFort include:

- **Risk Evaluation API**
- **Issuance API**

Risk Evaluation API

RiskFort SDK 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 also consists of the `Issuance` API package that enables the initial credential provisioning for users.

User management operations enabled by `Issuance API` include:

- Create user
- Update user

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 API 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*:

   `<install_location>/arcot/`

   to the appropriate location in your `<APP_SERVER_HOME>` directory. For example, for Apache Tomcat, this location is:

   `<Application_Home>/ROOT/WEB-INF/lib/`

   - `/sdk/java/lib/arcot/arcot_policy.jar`
   - `/sdk/java/lib/arcot/arcot_riskfort_sdk.jar`
   - `/sdk/java/lib/arcot/ArcotMFP.jar`
   - `/sdk/java/lib/external/json-lib-0.7.1.jar`
   - `/sdk/java/lib/external/servlet.jar`

2. Configure the `log4j.properties.riskfort_sdk` and `riskfort.properties` files:

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

  `<install_location>/arcot/sdk/java/properties/log4j.properties.riskfort_sdk`

  and

  `<install_location>/arcot/sdk/java/properties/riskfort.properties`

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

  I. Rename `log4j.properties.riskfort_sdk` to `log4j.properties`.

  II. Merge `riskfort.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/docs/Arcot-RiskFort-1.7-risk-evaluation-sdk-javadocs.tar.gz`.

Configuring Issuance Java API

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

Perform the following steps 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*:

   `<install_location>/arcot/`

   to the appropriate location in your `<APP_SERVER_ROOT>` directory. For example, for Apache Tomcat, this location is:

   `<Application_Home>/ROOT/WEB-INF/lib/`

   - `/sdk/java/lib/arcot/arcot_core.jar`
   - `/sdk/java/lib/arcot/arcot_riskfort_issuance.jar`
   - `/sdk/java/lib/external/bcprov-jdk14-131.jar`
   - `/sdk/java/lib/external/commons-beanutils.jar`
   - `/sdk/java/lib/external/commons-collections-3.1.jar`
   - `/sdk/java/lib/external/commons-digester.jar`
   - `/sdk/java/lib/external/commons-lang-2.0.jar`
   - `/sdk/java/lib/external/commons-logging.jar`
   - `/sdk/java/lib/external/commons-pool.jar`
   - `/sdk/java/lib/external/log4j-1.2.9.jar`
   - `/sdk/java/lib/external/sqljdbc.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/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/docs/Arcot-RiskFort-1.7-issuance-javadocs.tar.gz`.

Configuring Web Services

This section guides you through the steps for configuring the following RiskFort Web services:

- Configuring Risk Evaluation Web Service
- Configuring Issuance Web Service
- Configuring Administrative Web Service

Configuring Risk Evaluation Web Service

> **IMPORTANT:** Before proceeding with the configuration, ensure that the RiskFort Web service package was installed successfully during the RiskFort installation.

After the installation, **`arcotriskfortws.war`**, which provides the main **`ArcotRiskFortXActionWebService`** service, is available in the following folder:

`<install_location>/arcot/java/app/riskfort/`

You can install the `arcotriskfortws.war` file on any of the application servers mentioned in the "System Requirements" section.

Perform the following steps to configure the RiskFort Web service:

1. Stop the application server.
2. Deploy the `arcotriskfortws.war` file *from* the following directory to the appropriate location on your application server:

   `<install_location>/arcot/java/app/riskfort`

3. On the application server host, navigate to the following file:

   `<APP_SERVER_ROOT>\arcotriskfortws\WEB-INF\classes\properties\riskfortws.properties`

4. If required, change the value of the following parameters:
   - `riskfort.server.host` (The RiskFort Server IP address.)
   - `riskfort.server.port` (The RiskFort Server port at which it listens to the incoming requests.)
   - `riskfort.socket.connection_timeout`

- `riskfort.socket.connection_retries`
- `riskfort.socket.read_timeout`
- `riskfort.socketpool.maxactive`
- `riskfort.socketpool.useconnectionpooling`
- `riskfort.socketpool.timebetweenconnectioneviction`
- `riskfort.socketpool.idletimeofconnection`
- `riskfort.whenexhausted`

NOTE: Refer to "riskfort.properties" on page 157 to understand these parameters.

5. (Optional) Set the following parameters:
   - `TRANSPORT_TYPE=TLS` (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.properties" for more information on the configuration parameters.
6. Restart the application server.
7. In a browser window, check the following URL to verify the correct installation of the RiskFort Web Services:

   `http://<host>:<port>/arcotriskfortws/services/ArcotRiskFortXActionWebService`

Generating Client Code

The `riskfort` folder also contains the accompanying WSDLs that can be used to generate the Web Services client code to communicate with the RiskFort Web Services.

The generic steps to generate clients are:

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

   `<install_location>/arcot/java/app/riskfort/`
3. Use the following WSDLs to generate the client code:
   - `RiskFortXActionAPI.wsdl` **(for SOAP 1.2)**

- `RiskFortXActionAPISOAP11.wsdl` **(for SOAP 1.1)**

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://<APP_SERVER_IP>:<APP_SERVER_PORT>/arcotriskfortws/services/ArcotRiskFortXActionWebService`

   NOTE: To know more about Web Services, refer to the RiskFort WSDLdocs at `<install_location>/arcot/docs/Arcot-RiskFort-1.7-risk-evaluation-wsdldocs.tar.gz`.

Configuring Issuance Web Service

IMPORTANT: Before proceeding with the configuration, ensure that the Issuance Web service package was installed successfully during the RiskFort installation.

After the installation, **`arcotriskfortissuancews.war`**, which provides the main **`User`** service for issuance-related activites, is available in the following folder:

`<install_location>/arcot/java/app/riskfort/`

You can install the `arcotriskfortissuancews.war` file on any of the application servers mentioned in the "System Requirements" section.

Perform the following tasks to configure the Issuance Web service:

1. Stop the application server.
2. Copy the file `arcotriskfortissuancews.war` *from:*

   `<install_location>/arcot/java/app/riskfort/`

   to the appropriate location in your `<APP_SERVER_HOME>` directory.

   Here, *`APP_SERVER_HOME`* represents the directory path where application server (for example, Apache Tomcat) is installed.
3. On the application server host, navigate to the following file:

   `<APP_SERVER_ROOT>\arcotriskfortws\WEB-INF\classes\properties\riskfort_issuance.properties`
4. If required, change the value of the following parameters:

- `HOST1` (The RiskFort Server IP address.)
- `PORT1` (The RiskFort Server port at which it listens to the incoming Issuance requests.)
- `CONNECTION_TIMEOUT`
- `CONNECTION_RETRIES`
- `READ_TIMEOUT`
- `USE_CONNECTION_POOLING`
- `MAX_ACTIVE`
- `TIME_BETWEEN_CONNECTION_EVICTION`
- `IDLE_TIME_OF_CONNECTION`
- `WHEN_EXHAUSTED_ACTION`

NOTE: Refer to "riskfort_issuance.properties" on page 159 to understand these parameters.

5. (Optional) Set the following parameters:
   - `TRANSPORT_TYPE=TLS` (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.
6. Restart the application server.
7. In a browser window, access the following URL to verify if the client can access the Web Service:

   `http://<APP_SERVER_IP>:<APP_SERVER_PORT>/arcotriskfortissuancews/services/ArcotRiskFortIssuanceWebService`

Generating Client Code

The `riskfort` folder also contains the accompanying WSDLs (**`RiskFortIssuanceAPI.wsdl`**) that can be used to generate the Web Services client code to communicate with RiskFort Web Services.

The generic steps to generate clients are:

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

   `<install_location>/arcot/java/app/riskfort/`

3. Use the following WSDLs to generate the client code:
   - `RiskFortIssuanceAPI.wsdl` (**for SOAP 1.2**)
   - `RiskFortIssuanceAPISOAP11.wsdl` (**for SOAP 1.1**)
4. Restart the application server.

   NOTE: To know more about Web Services, refer to the Issuance WSDLdocs at `<install_location>/arcot/docs/Arcot-RiskFort-1.7-issuance-wsdldocs.tar.gz`.

Configuring Administrative Web Service

IMPORTANT: Before proceeding with the configuration, ensure that the Admin Web service package was installed successfully during the RiskFort installation.

After the installation, **`ArcotRiskFortAdminWebService.war`**, which provides the RiskFort administrative services, is available in the following location:

`<install_location>/arcot/java/app/admin/`

You can install the `ArcotRiskFortAdminWebService.war` file on any of the application servers mentioned in the "System Requirements" section.

Perform the following steps to configure the RiskFort administrative Web service:

1. Stop the application server.
2. Copy the `ArcotRiskFortAdminWebService.war` file *from* the following directory:

   `<install_location>/arcot/java/app/admin/`

   to the appropriate location in your `<APP_SERVER_HOME>` directory.

   Here, *`APP_SERVER_HOME`* represents the directory path where application server (for example, Apache Tomcat) is installed.
3. Restart the application server.

4. Check the following URLs to verify the correct installation of the RiskFort Web Services:

   - **List service**

     `http://app_server_host:port/ArcotRiskFortAdminWebService/services/listServices`

   - **Exception user service**

     `http://app_server_host:port/ArcotRiskFortAdminWebService/services/ExceptionUserService`

   - **Administrative service**

     `http://app_server_host:port/ArcotRiskFortAdminWebService/services/ArcotAdminWebService`

Generating Client Code

The `admin` folder 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 generic steps to generate clients are:

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

   `<install_location>/arcot/java/app/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://<APP_SERVER_IP>:<APP_SERVER_PORT>/ArcotRiskFortAdminWebService/services/ArcotAdminWebService`

Configuring Device ID Cookies

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 cookie.

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

- **Configuring HTTP Cookies**
- **Configuring Flash Cookies**

Configuring HTTP Cookies

When you perform Complete installation (see **"Performing Complete Installation"** for more information) or select to install RiskFort Evaluation SDK or Web Service in the Choose Install Set screen (see **Step 11 on page 70** for more information), the following file is automatically installed:

`<install_location>/arcot/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 folder 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 Cookies

When you perform Complete installation (see **"Performing Complete Installation"** for more information) or select to install RiskFort Evaluation SDK or Web Service in the Choose Install Set screen (see **Step 11 on page 70** 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/sdk/javascript/rfutil.js`

This file provides JavaScript functions to get and set the Flash cookies for Device ID. In addition, this file also provides JavaScript functions to load `rfdevice.swf`.

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

rfdevice.swf

This file is installed at the following location:

`<install_location>/arcot/sdk/flash/rfdevice.swf`

This file manges Flash cookies 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/sdk/flash/crossdomain.txt`

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

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 Cookie Configuration

To configure for a Flash cookie 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 cookies.

   a. Copy `rfutil.js` to an appropriate Web application folder 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 folder.

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

3. If your Flash cookie 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`.

Chapter 7

Uninstalling RiskFort

This chapter guides you through the steps for uninstalling RiskFort and related components.

The steps to uninstall RiskFort are:

1. **Removing the Database**
2. **Uninstalling RiskFort Server**
3. **Performing Post-Uninstallation Tasks**

> **IMPORTANT:** If you have more than one Arcot products installed on your system, then you must ensure that the uninstallation follows the Last In First Out (LIFO) model. In other words, the product that you installed last must be uninstalled first.

Removing the Database

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.

Perform the following tasks to uninstall the database:

1. Navigate to the following directory:

For Oracle: `<install_location>/arcot/dbscripts/oracle/`

2. Run the following scripts *in the order specified below* to drop the database tables:
   - `drop-riskfort-1.7.sql`
   - `drop-webfort-5.4.1.sql`
   - `drop-arcot-common-1.0.sql`

Uninstalling RiskFort Server

To uninstall RiskFort Server, you need to remove the files shipped with RiskFort. Uninstallation also deletes the scripts required to uninstall the database. If you need to remove the RiskFort database, then refer to "Removing the Database" section before proceeding.

Perform the following tasks to uninstall RiskFort Server:

1. Shut down the following components gracefully:
   - WebFort Server
   - RiskFort Server
   - Administration Console
   - Any application servers where other RiskFort components are deployed
2. Ensure that all INI and other files related to RiskFort are closed.
3. Use the following command to uninstall **WebFort Basic**:

   ```
   prompt><install_directory>/arcot/"Uninstall Arcot WebFort
   5.4.1"/Uninstall_Arcot_WebFort_5.4.1
   ```

4. Use the following command to start the uninstallation of **RiskFort**:

   ```
   prompt><install_directory>/arcot/"Uninstall Arcot RiskFort
   1.7"/Uninstall_Arcot_RiskFort_1.7
   ```

   The Uninstall Arcot RiskFort screen appears.
5. Press **Enter** to confirm and continue with the uninstallation. This might take several minutes.

   After the uninstallation is completed, the Uninstall Complete screen appears and you are returned to the command prompt.

Performing Post-Uninstallation Tasks

The following are the post uninstallation steps:

1. Delete the directories from `<install_location>/arcot/`, if not required after uninstallation.

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

2. Uninstall the following WAR files from the appropriate subdirectory in your `<APP-SERVER-HOME>` directory:

   NOTE: Refer to the application server vendor documentation for detailed information on uninstalling the WAR files.

   - `arcotadmin.war`
   - `arcotriskfortws.war`

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

3. Delete the file `tabspace_arrfreports.dat` from the computer running the database server.

4. Delete the DSN entry created during the RiskFort installation.

   To delete this entry, navigate to the `odbc.ini` file, open it by using a text editor, and delete the corresponding database entry. Based on your ODBC setup, this file might be available at *one* of the following locations:

   - `/etc/odbc.ini`
   - `/usr/local/etc/odbc.ini`

Appendix A

RiskFort Directory Structure

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

> **IMPORTANT:** In addition to the files and directories discussed in "Directory Structure", you will also see a blank file called **`arcotkey`** in the `arcot` 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.

Directory Structure

The following table 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.

Table A-1 Installation Directory Structure for Linux

Directory	File Description
`<install_location>/arcot/bin/`	Contains the following executable files: • `aradmin` (Tool for refreshing and gracefully shutting down the RiskFort Server.) • `ArcotRiskFortServer` (RiskFort Server binary.) • `ArcotWebFortServer` (WebFort Server binary. **Note:** This file is available only *after* you install WebFort.) • `arversion` (Tool for determining the version of the modules provided by Arcot.) • `DBUtil` (Tool for editing the `secure-store.enc` file that stores encrypted information needed to connect to the RiskFort database.) • `arrfupload` (Tool for uploading Quova data to RiskFort database.) **NOTE:** See *Arcot RiskFort Administration Guide* for more details on `aradmin`, `arversion`, `DBUtil`, and `arrfupload` tools.
`<install_location>/arcot/certs/`	Container for all server certificates.

Table A-1 Installation Directory Structure for Linux

Directory	File Description
<*install_location*>/arcot/conf/	Contains the following configuration files: • adminserver.ini • arcotcommon.ini • jni.ini • regfort.ini • riskfortserver.ini • securestore.enc • webfortserver.ini (**Note:** This file is available only *after* you install WebFort Basic.) **NOTE:** See Appendix C, "Configuration Files and Options for more details on server configuration files.
<*install_location*>/arcot/db-scripts/	Contains the required Oracle database scripts to create the RiskFort schema. **NOTE:** The directories created in this location depends on the DSN Type that you selected during the installation.
<*install_location*>/arcot/docs/	Contains Javadocs and WSDLdocs for: • RiskFort Risk Evaluation and Issuance • Admin Web Services • XSDs required for writing Callouts
<*install_location*>/arcot/il8n/	Contains the files required for internationalization of WebFort. **NOTE:** This directory is available only *after* you install WebFort Basic.

Table A-1 Installation Directory Structure for Linux

Directory	File Description
<*install_location*>/arcot/java/app/	Contains the WAR and WSDL files required by RiskFort and the Administration Console. The subdirectory **admin** contains the following files: • arcotadmin.war (The WAR file required to deploy the Administration Console.) • arcotadminws.war (The deprecated WAR file for deploying the ExceptionUser Web Service.) • ArcotRiskFortAdminWebService.war (The WAR file required to deploy the Admin Web Services shipped in this release.) • ArcotRiskFortAdminWebService.wsdl (The WSDLdoc that describes the Admin Web Services and how to access them.) • ExceptionUserService.wsdl (The WSDLdoc that describes the deprecated ExceptionUser Web Services and how to access them.) The subdirectory **riskfort** contains : • arcotriskfortissuancews.war (The WAR file required to deploy Issuance.) • arcotriskfortws.war (The WAR file required to deploy RiskFort Transaction Web service APIs.) • RiskFortIssuanceAPI.wsdl (The WSDLdoc that describes the arcotriskfortissuancews Web Services and how to access them.) • RiskFortXActionAPI.wsdl (The WSDL document corresponding to the older Risk Evaluation APIs.) • RiskFortXActionAPIEx.wsdl (The WSDL document corresponding to new Risk Evaluation APIs.) • RiskFortXActionAPISOAP11.wsdl

Table A-1 Installation Directory Structure for Linux

Directory	File Description
<*install_location*>/arcot/lib/	Contains RiskFort Server binaries, such as: • aradmincsdk.so • ArcotJNICreateCard.so • arRiskEngine.so • NameValueXref.so The directory also contains the **admin** subdirectory with the ArcotJNICreateCard.so file.
<*install_location*>/arcot/logs/	Contains the installation and other log files.
<*install_location*>/arcot/plugins/	Contains the framework, mechanisms, protocols, rules, and tokengenerators directories. • The framework directory contains WebFortFramework.so. • The issuance folder contains issuance.so. • The mechanisms directory contains authentication-related binaries. • The **protocols** directory contains the binaries for Server Management and Native protocols used by the Administration Console. • The **rules** directory contains the binary files to support out-of-box Riskfort rules and Scoring. • The **rules/addon** directory *must* contain the .so files for all Add-On rules, if you deploy one or more of these custom rules. • The tokengenerators directory contains otptoken.so.

Table A-1 Installation Directory Structure for Linux

Directory	File Description
`<install_location>/arcot/samples/java/`	Contains the WAR files for: • RiskFort Sample Application • RiskFort Sample Callouts **NOTE:** See the *Arcot RiskFort 1.7 Administration Guide* for more information on Callouts and how to deploy the Sample Callout shipped with RiskFort.

Table A-1 Installation Directory Structure for Linux

Directory	File Description

<*install_location*>/arcot/sdk/	Contains SDKs and dependant files supported by RiskFort.
	• The **c** folder contains the library and included files required for C SDK.
	• The **flash** directory contains:
	  • crossdomain.txt, which specifies the list of domains that can access the Flash cookie.
	  • rfdevice.swf, which manages the the Device ID Flash cookie.
	• The **java/lib** directory contains the Arcot-supplied and third-party JAR files.
	• The **java/properties** directory contains the following property files required for configuration of RiskFort:
	  • log4j.properties.issuance
	  • log4j.properties.riskfort_sdk
	  • riskfort.properties
	• The **javascript** directory contains:
	  • mfp.json, which is required at the client-end for collecting Machine FingerPrint (MFP) information.
	  • rfutil.js, which is required to get and set Flash cookies and load rfdevice.swf in the flash directory.

<*install_location*>/arcot/tools/	Contains the Opensslca tool for generating OpenSSL certificates.
<*install_location*>/arcot/Uninstall Arcot RiskFort 1.7/	Contains the files required to uninstall RiskFort.

Table A-1 Installation Directory Structure for Linux

Directory	File Description
<*install_location*>/arcot/Uninstall Arcot RiskFort 1.7/jre	Contains all files required for Java Runtime Environment (JRE) support. These include: • Java Virtual Machine • Runtime Class Libraries • Java Application Launcher
<*install_location*>/arcot/Uninstall Arcot WebFort 5.4.1/	Contains the files required to uninstall WebFort. **NOTE:** This directory is available only after you install WebFort Basic.

Appendix B

Installing RiskFort with Complete WebFort Functionality

Typically, you will install RiskFort *first* and *then* install WebFort **Basic**, which RiskFort uses for authenticating administrators to the Administration Console. However, you might want to avail the complete functionality of WebFort. In this case, follow the instructions in this appendix to install RiskFort with complete installation of WebFort.

This chapter covers the instructions for installing RiskFort with complete WebFort functionality in the following environments:

- **Single-System Installation**
- **Distributed-System Installation**

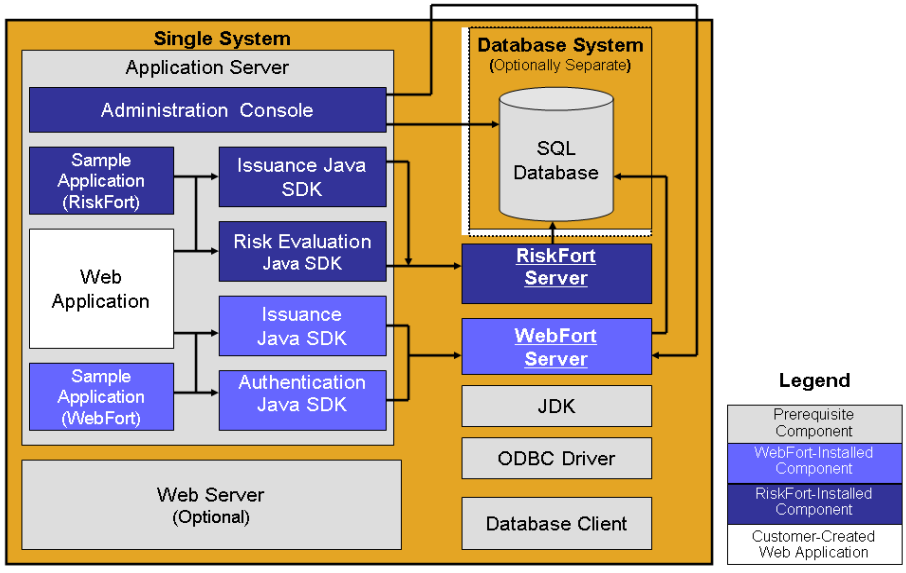
Single-System Installation

In a single-system deployment, all components of WebFort, RiskFort, and your 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. It is possible to use both Java SDKs and Web Services in a single-system deployment. The prerequisite software for these components are identical.

Typically, if you are only using RiskFort, then you install RiskFort first and then install WebFort Basic. However if you would like to use the complete WebFort functionality along with RiskFort, then you must first install WebFort and then RiskFort. The simplest way to perform a single-system deployment is to choose the **Complete Installation** option while running the WebFort and RiskFort installers.

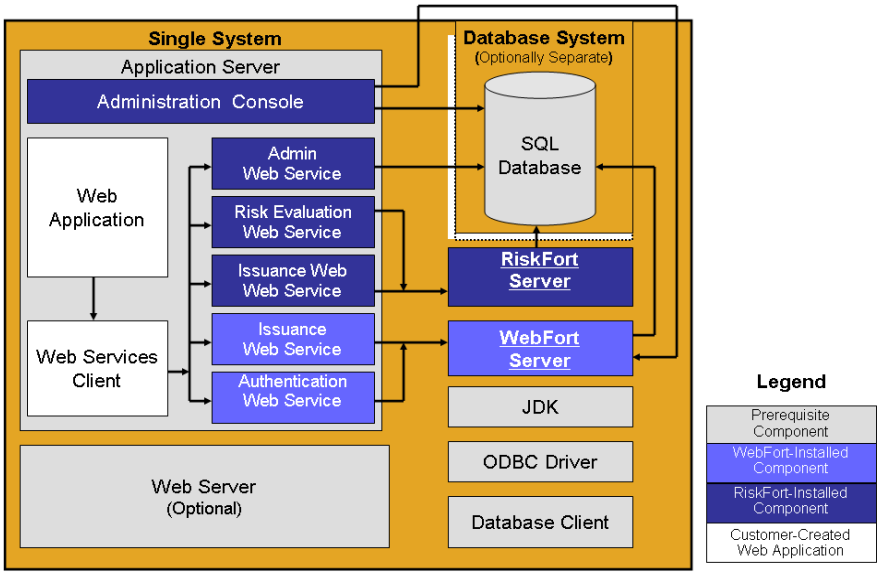
The following figure illustrates RiskFort Server, WebFort Server, and Java SDKs for RiskFort and WebFort deployed on a single system.

Figure B-1



The following figure illustrates RiskFort Server, WebFort Server, and Web Services for RiskFort and WebFort deployed on a single system.

Figure B-2



To install WebFort and RiskFort components on the same computer:

- Step 1: WebFort Complete Installation
- Step 2: RiskFort Complete Installation
- Step 3: Post-Installation Tasks

Step 1: WebFort Complete Installation

To install and configure WebFort components:

1. Navigate to the directory where the `Arcot-WebFort-5.4.1-Linux-Installer.bin` file is located and double-click the file to run the installation wizard.
2. Follow the instructions on the wizard screens to install. On the Type of Installation screen, you must select the **Complete** option.

   See "**Installing WebFort**" in Chapter 4, "Deploying WebFort on a Single System" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

3. Execute the database scripts (**`arcot-db-initial-config-common-1.0.sql`** and then **`arcot-db-config-for-webfort-5.4.1.sql`**) to create WebFort schema and database tables.

   See "**Running Database Scripts**" in Chapter 4, "Deploying WebFort on a Single System" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

4. Run the command-line utility, **`openssl`**, to configure Arcot's private OpenSSLCA.

   See "**Configuring OpenSSLCA**" in Chapter 4, "Deploying WebFort on a Single System" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

Step 2: RiskFort Complete Installation

To install and configure RiskFort components:

1. Navigate to the directory where the `Arcot-RiskFort-1.7-Linux-Installer.bin` file is located and double-click the file to run the installation wizard.

2. Follow the instructions on the wizard screens to install. On the Type of Installation screen, you must select the **Complete** option.

   See "Performing Complete Installation" on page 37 for detailed instructions.

   IMPORTANT: *Do not* install WebFort Basic (Step 20 on page 41), because WebFort Complete has already been installed, as discussed earlier.

3. Execute the RiskFort database script to create RiskFort schema and database tables. Also ensure that the database setup was successful:

   a. Navigate to the following folder:

      `<install_location>/arcot/dbscripts/oracle/`

   b. Run the **`arcot-db-config-for-riskfort-1.7.sql`** script.

   c. Verify whether the database was set up correctly.

      See "Verifying the Database Setup" on page 44 for more information.

4. Test the installation.

   See "Verifying the Installation" on page 44 for detailed instructions.

5. Deploy Administration Console on the application server and verify the deployment.

   See "Deploying Administration Console" on page 46 and "Verifying the Administration Console Deployment" on page 47 for more information.

Step 3: Post-Installation Tasks

To complete configuration of RiskFort and WebFort:

1. Log in to Administration Console with the Master Administrator credentials to:

   a. Initialize RiskFort and WebFort.

      See "Logging in to Administration Console" on page 48 for more information.

   b. Create a Domain Key in WebFort.

      See **"Creating a Domain Key"** in Chapter 4, "Deploying WebFort on a Single System" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

   c. Create a Global Administrator.

      See "Creating a Global Administrator" on page 49 for more information.

2. Optionally, to ensure secure communication between RiskFort components, you can configure them to support TLS (Transport Layer Security) transport mode. This is an optional step.

   See "(Optional) Configuring TLS Communication Mode" on page 52 for more information.

3. Optionally, configure TLS communication between WebFort Server and its components.

   See "**Configuring TLS Communication**" in Chapter 4, "Deploying WebFort on a Single System" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

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

   See "Deploying Sample Application" on page 61 and "Using Sample Application" on page 63 for more information.

5. Deploy Sample Application for testing WebFort. The Sample Application is also used as a code sample for integrating ArcotID authentication to your existing Web applications.

   See "**Deploying Sample Application**", "**Configuring Sample Application for WebFort Server**", and "**Using Sample Application**" in Chapter 4, "Deploying WebFort on a Single System" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

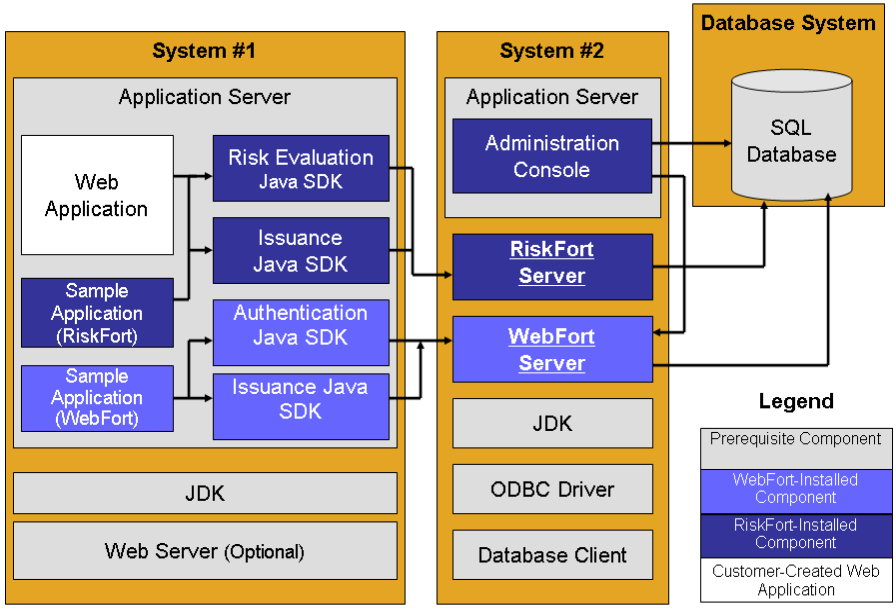
Distributed-System Installation

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

For example, the most common deployment is to install RiskFort Server, WebFort Server, and Administration Console on one system (secured behind a load balancer and/or a firewall) and the RiskFort and WebFort SDKs, along with one or more Web applications on additional systems.

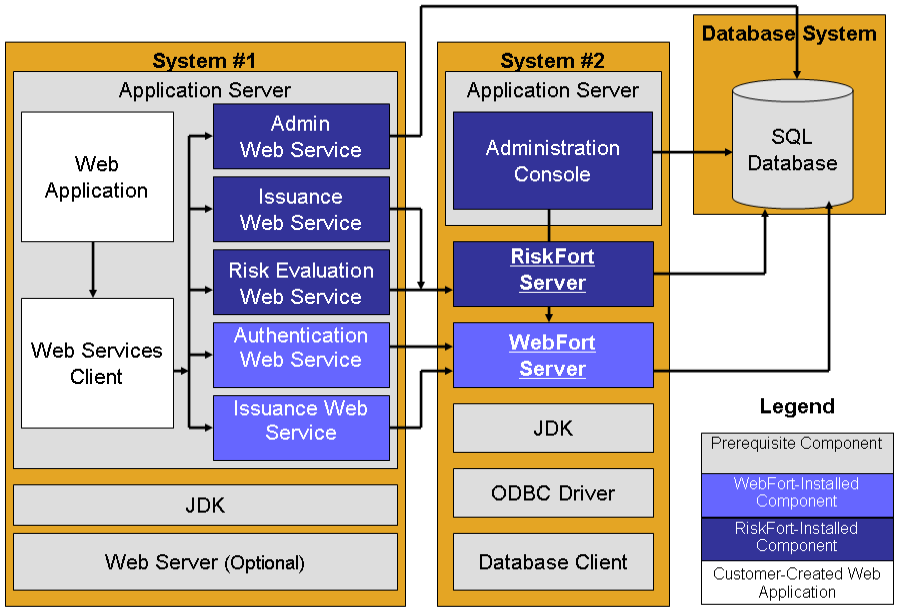
The following figure illustrates the typical deployment of RiskFort Server and WebFort Server using Java SDKs (for RiskFort and WebFort) with a single Web application. You can deploy multiple Web applications, if required.

Figure B-3



The following figure illustrates RiskFort Server and WebFort Server using Web Services (for RiskFort and WebFort) with a single Web application. You can deploy multiple Web applications, if required.

Figure B-4



Typically if you are only using RiskFort, then you install RiskFort first and then install WebFort Basic. However if you would like to use the complete WebFort functionality along with RiskFort, then you must first install WebFort and then RiskFort. To perform a distributed-system deployment you must select the **Custom** installation option while running the WebFort and RiskFort installers.

To install WebFort and RiskFort components on multiple computers:

- Step 1: Install and Configure WebFort Components On the First System
- Step 2: Install and Configure WebFort Components on the Second System
- Step 3: Install and Configure RiskFort Components On the First System
- Step 4: Install and Configure RiskFort Components on the Second System
- Step 5: Perform Post-Installation Tasks on the Second System

Step 1: Install and Configure WebFort Components On the First System

To install selected WebFort components, create the WebFort schema in the database, and generate new Issuer Root keypair and certificate:

1. Navigate to the directory where the `Arcot-WebFort-5.4.1-Linux-Installer.bin` file is located and double-click the file to run the installation wizard.
2. Follow the instructions on the wizard screens to install:
   - On the Type of Installation screen, you must select the **Custom** option.
   - On the Choose Install Set screen, deselect the components that are not required.

     For example, to install WebFort Server and Administration Console on the current system, you will need to:

     I. Select the main **WebFort Authentication** option and under it, select **WebFort Server** option.

     II. Deselect **Authentication SDK** and **Authentication Web Service** components.

     III. Deselect **Issuance**, **Issuance SDK**, and **Issuance Web Service** components.

     IV. Select the **Administration Console** option.

   See "**Installing WebFort**" in Chapter 5, "Deploying WebFort on Distributed Systems" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.
3. Execute the database scripts (**`arcot-db-initial-config-common-1.0.sql`** and then **`arcot-db-config-for-webfort-5.4.1.sql`**) to create WebFort schema and database tables.

   See "**Running Database Scripts**" in Chapter 5, "Deploying WebFort on Distributed Systems" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.
4. Run the command-line utility, **`openssl`**, to configure Arcot's private OpenSSLCA.

   See "**Configuring OpenSSLCA**" in Chapter 5, "Deploying WebFort on Distributed Systems" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

Step 2: Install and Configure WebFort Components on the Second System

To install selected WebFort components and configure them to communicate with WebFort Server:

1. Install the required SDKs and Web Services on one or more systems. Typically, you will be installing the Java SDKs or the Web Services for Authentication and Issuance.

   On the Choose Install Set screen, select only the SDK or Web Services component that you want to install and ensure that other components are deselected.

   > **NOTE:** In case of Issuance SDK or Web Services components, you *must* select the main **Issuance** option as well.

   See "**Installing on Second System**" in Chapter 5, "Deploying WebFort on Distributed Systems" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

2. For each computer where you installed the WebFort SDK or Web Services, copy the configuration files *from* the first system where WebFort Server is installed *to* the system where SDKs are installed.

   See "**Copying Configuration Files**" in Chapter 5, "Deploying WebFort on Distributed Systems" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

Step 3: Install and Configure RiskFort Components On the First System

To install selected RiskFort components, create the RiskFort schema in the database, and deploy the Administration Console:

1. Navigate to the directory where the `Arcot-RiskFort-1.7-Linux-Installer.bin` file is located and double-click the file to run the installation wizard.
2. Follow the instructions on the wizard screens to install:
   - On the Type of Installation screen, you must select the **Custom** option.
   - On the Choose Install Set screen, deselect the components that are not required.

     For example, to install RiskFort Server and Administration Console on the current system, you will need to:

     I. Select the main **Risk Evaluation** option and under it, select the **RiskFort Server** option.

II. Deselect **Risk Evaluation SDK** and **Risk Evaluation Web Service** components.

III. Deselect **Issuance**, **Issuance SDK**, and **Issuance Web Service** components.

IV. Select the **Administration Console** option.

See "Installing on the First System" on page 69 for detailed instructions.

IMPORTANT: Do not install WebFort Basic (Step 22 on page 74), because WebFort components have already been installed, as discussed in the previous section.

3. Execute the RiskFort database script to create RiskFort schema and database tables. Also ensure that the database setup was successful:

   a. Navigate to the following folder:

      `<install_location>/arcot/dbscripts/oracle/`

   b. Run the **`arcot-db-config-for-riskfort-1.7.sql`** script.

   c. Verify whether the database was set up correctly.

      See "Verifying the Database Setup" on page 77 for more information.

4. Test the installation.

   See "Verifying the Installation" on page 77 for detailed instructions.

5. Deploy Administration Console on the application server and verify the deployment.

   See "Deploying Administration Console" on page 79 and "Verifying the Administration Console Deployment" on page 80 for more information.

Step 4: Install and Configure RiskFort Components on the Second System

To install selected RiskFort components and configure them to communicate with RiskFort Server:

1. Install the required SDKs and Web Services on one or more systems. Typically, you will be installing the Java SDKs or the Web Services for Risk Evaluation and Issuance.

   On the Choose Install Set screen, select only the SDK or Web Services component that you want to install and ensure that other components are deselected.

> **NOTE:** In case of Issuance SDK or Web Services components, you *must* select the main **Issuance** option as well.

See "Installing on the Second System" on page 92 for more information.

2. Optionally, to ensure secure communication between RiskFort components, you can configure them to support TLS (Transport Layer Security) transport mode. This is an optional step.

   See "(Optional) Configuring TLS Communication" on page 85 for more information.

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

   > **NOTE:** Sample Application is automatically installed as a part of Complete installation.

   See "Deploying Sample Application" on page 87, "Configuring Sample Application for Communication with RiskFort Server" on page 88, and "Using Sample Application" on page 89 for more information.

Step 5: Perform Post-Installation Tasks on the Second System

To ensure communication between the distributed components of RiskFort and WebFort:

1. Optionally, configure TLS communication between WebFort Server and its components.

   See "**Configuring TLS Communication**" in Chapter 5, "Deploying WebFort on Distributed Systems" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

2. Deploy Sample Application for testing WebFort. The Sample Application is also used as a code sample for integrating ArcotID authentication to your existing Web applications.

   See "**Deploying Sample Application**", "**Configuring Sample Application for WebFort Server**", and "**Using Sample Application**" in Chapter 5, "Deploying WebFort on Distributed Systems" of the *Arcot WebFort Installation and Deployment Guide* for detailed instructions.

Appendix C

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 are:

- **arcotcommon.ini**
- **riskfortserver.ini**
- **adminserver.ini**
- **regfort.ini**
- **jni.ini**
- **riskfort.properties**
- **riskfort_issuance.properties**
- **log4j.properties.riskfort_sdk**
- **log4j.properties.riskfort_issuance**

The chapter also provides a default sample of all RiskFort configuration files in section, **"Sample Configuration Files."**

All RiskFort configuration files are available at the following default location:

`<install_location>/arcot/conf/`

arcotcommon.ini

Typically, you might need to edit the following sections in the `arcotcommon.ini` file:

- **Database Setting Parameters**
- **Instance Settings**

Refer to the **"Sample Configuration Files"** section for the default sample content of this file.

Database Setting Parameters

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.

For notes and recommendations for database settings, refer to the **"Configuring Database Server"** section in **Chapter 3.**

You must edit the following sections related to database settings in the `arcotcommon.ini` file:

- **The [arcot/db/dbconfig] Section**
- **The [arcot/db/primarydb] Section**
- **The [arcot/db/backupdb] Section**

The [arcot/db/dbconfig] Section

This section allows you to specify the type of the database (Oracle) and generic information about this database type.

The following table lists the database setting parameters in the `[arcot/db/dbconfig]` section.

Table C-1 Database Setting Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
`DbType`	`oracle`	The type of the database applicable to all database connections. The supported values are: • `oracle`

Table C-1 Database Setting Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
`Driver`	No default	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`
`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 database driver manual for more information about the limit on number of inbound connections.
`MinConnections`	`16`	The minimum number of connections to initially create between the server and the database.
`IncConnections`	`4`	The number of connections that will be created when a new connection is needed between the server and the database.
`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.
`ConnRetrySleepTime`	`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`	The database messages are being logged. Set to 1 if you want to enable logging of database messages.

Table C-1 Database Setting Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
`EnableBrandLicensing`	`0`	Whether a branded ODBC driver is in use. This can be used when you are using the branded ODBC drivers from Data Direct.
`BrandLicenseFile`	*<license_file_name>*	The license file name when you use a branded ODBC driver.
`MaxTransactionRetries`	`3`	The maximum number of times the transaction is retried with a database instance for pre-defined error conditions.
`TransactionRetrySleepTime`	`10`	The interval in **milliseconds** between two consecutive transaction retries.

The [arcot/db/primarydb] Section

This section allows you to specify the primary database to which the RiskFort Server will be connected to. You can configure more than one primary databases by specifying the required number, `N` in the following parameters:

- `Datasource.<N>`
- `Username.<N>`
- `URL.<N>`

The following table lists the database setting parameters in the `[arcot/db/primarydb]` section.

Table C-2 Primary Database Parameters in the `[arcot/db/dbconfig]` Section

Parameter	Default	Description
`Datasource.<N>`	`Arcot<`*`ServerName`*`>Database`	The name of the ODBC System Data Source Name (DSN) pointing to the primary database hosting the server data.
`URL.<N>`	No default	The name of the JDBC data source. For • Oracle -> `jdbc:oracle:thin:<server>:<`*`port`*`>:<sid>` • SQLServer -> `jdbc:sqlserver://<server>:<`*`port`*`>;databaseName=<databasename>;selectMethod=cursor`
`Username.<N>`	No default	The user ID used by the server to access the database.

The [arcot/db/backupdb] Section

This section allows 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>`
- `Username.<N>`
- `URL.<N>`

This section uses the same parameters as the **"The [arcot/db/primarydb] Section,"** section. Refer to **Table C-2** for the list of the database setting parameters in the `[arcot/db/backupdb]` 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 allows you to configure these system-wide settings for unique instances.

The following table lists the instance setting parameters in the `[arcot/system]` section

Table C-3 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.

riskfortserver.ini

By using the `riskfortserver.ini` file, you can configure the following settings:

- Log File Settings
- Thread Settings

Refer to the "Sample Configuration Files" section for the default sample content of this file.

Log File Settings

RiskFort records all system actions in the `arcotriskfort.log` file. The default location of this file is:

`<install_location>/arcot/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. The following table lists the log file setting parameters in the `riskfortserver.ini` files and provides descriptions of each:

Table C-4 Log File Parameters in riskfortserver.ini

Parameter	Default	Description
`Logfile`	`logs/arcotriskfort.log` **Note:** This path is relative to `<install_location>/arcot/`	The file path to the default directory and the file name of the log file.
`LogfileSize`	`10485760`	The maximum number of bytes the log file can contain. When the log files reach this size, a new file is started and the old file is moved to the `BackupLogFileDir`.

Table C-4 Log File Parameters in riskfortserver.ini

Parameter	Default	Description
BackupLogFileDir	logs/backup **Note:** This path is relative to <install_location>/arcot/	The location of the directory where backup log files are maintained after the current one exceeds LogFileSize bytes.
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

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. The following table lists the thread setting parameters in the `ini` files and provides descriptions of each:

Table C-5 Thread Setting Parameters

Parameter	Default	Description
`MaxThreads`	`128`	The maximum number of threads that the server can maintain. This has a direct impact on the number of concurrent requests the server can process.
`MinThreads`	`32`	The minimum number of threads that the server must maintain.

adminserver.ini

The `adminserver.ini` file specifies the parameters for:

- Authentication Settings
- External Settings

Refer to the "Sample Configuration Files" section for the default sample content of this file.

Authentication Settings

You can configure the location at which the authentication server is available by editing the parameters (discussed in the following table) in the `[arcot/admin/authconfig]` section.

Table C-6 Parameters for Authentication Settings in adminserver.ini

Parameter	Default	Description
`remotehost.1`	*<Authentication server IP Address>*	Internet Protocol (IP) address at which WebFort Server is available.
`remoteport.1`	`9742`	Port at which WebFort Server is listening to incoming requests.
`transport`	`TCP`	Default value for Administration Console to start up is TCP. Set this parameter to **TLS**, if RiskFort Native protocol is set to TLS. In other words, set this parameter to TLS if you want to enable TLS-based secure communication between Administration Console and WebFort Server. **NOTE:** You *must* restart WebFort Server and Administration Console, if you change the value to `TLS`.

Table C-6 Parameters for Authentication Settings in adminserver.ini

Parameter	Default	Description
server.CACert	*<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/webfort_ca.pem

External Settings

You can configure the external settings, such as login URL, group enrollment link, server information, and JNI library path by editing the parameters (listed in the following table) in the [arcot/admin/config] section.

Table C-7 External Settings Parameters in adminserver.ini

Parameter	Default	Description
groupEnrollmentLink	*<https://<HostServerName>:<HostServerPortNo>/enroll/index.htm?sgid=>*	The user enrollment link for a group.
LOGIN_URL_PATH	*<http://<HostServerName>:<HostServerPortNo>/arcotadmin>*	The URL which is used to log in to the Administration Console.
serverInfo	*<HostServerIPAddress>:<HostServerPortNo>*	The information of the server that Administration Console accesses to generate the reports.
JNI_LIBRARY_PATH	No Default	The path where the JNI libraries delivered with the Arcot application are available.

regfort.ini

The `regfort.ini` file contains the parameter for configuring the JNI library path. You can configure this parameter under the `[arcot/regfort/config]` section.

The following table describes the all the parameters.

Table C-8 Parameter for JNI Configuration

Parameter	Default	Description
`JNI_LIBRARY_PATH`	No default value	Specifies the path where the JNI libraries delivered with Arcot application is present. **Note:** You *must* ensure that this path is different from the JNI library path for Administration Console.

jni.ini

The `jni.ini` file contains parameters for the following configuration:

- **Log File Settings**
- **Configuration for Administration Console**
- **Configuration for Administration Console**
- **Configuration for Administration Console**

Log File Settings

JNI records all system actions that have occurred in the `arcotjni.log` file. The default location of this file is:

`<install_location>/arcot/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. After the primary log file reaches the maximum size, the system will then record new actions in a new log file, which will be a new instance of `arcotjni.log`.

All logging-related parameters are the `[arcot/jni/logger]` section in the `jni.ini` file.

The following table lists the log file setting parameters in the `jni.ini` file and provides descriptions of each.

Table C-9 Log File Parameters in jni.ini

Parameter	Default	Description
`Logfile`	`logs/arcotjni.log` **Note:** This path is relative to `<install_location>/arcot/`	The file path to the default directory and the file name of the log file.
`LogfileSize`	`10485760`	The maximum number of bytes the log file can contain. When the log files reach this size, a new file is started and the old file is moved to the `BackupLogFileDir`.

Table C-9 Log File Parameters in jni.ini

Parameter	Default	Description
BackupLog-FileDir	logs/backup **Note:** This path is relative to <install_location>/arcot/	The location of the directory where backup log files are maintained after the current file exceeds LogFileSize bytes.
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
CreateLog	1	The parameter that indicates whether the logging is enabled or not. The possible values are: • 0 OFF • 1 ON

Configuration for Administration Console

The parameters required for the Administration Console are configured under the section [arcot/jni/admin] in the jni.ini file.

The following table lists the parameters and provides descriptions of all parameters required for configuration of Administration Console.

Table C-10 Parameters for Administration Console Configuration in jni.ini

Parameter	Default	Description
CertDirectory	certs/certif-icates **Note:** This path is relative to <install_location>/arcot/	Default directory where the domain and RA certificates generated by the CA are stored.

Table C-10 Parameters for Administration Console Configuration in jni.ini

Parameter	Default	Description
RAStore	certs/p12stores/ras-tore.p12 **Note:** This path is relative to <install_location>/arcot/	When Administration Console requests RA store creation, the RA's private key and certificate are stored in this file. This is also used by Issuance to obtain the RA store location.
DomainStore	certs/p12stores/domainkey-store.p12 **Note:** This path is relative to <install_location>/arcot/	When Administration Console requests domain key/certificate creation, the key is created and stored in this file.

Properties Files

RiskFort primarily uses the two properties files discussed in the following sub-sections. These files are available at:

`<install_location>/arcot/sdk/java/properties/`

riskfort.properties

The `riskfort.properties` file provides the parameters for the Java SDK and Sample Application to read RiskFort Server information. The following table lists the configuration parameters..

Table C-11 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	3	Maximum number of retries allowed with RiskFort Server.
READ_TIMEOUT	30000	Maximum time in **milliseconds** allowed for a response from RiskFort Server.
USE_CONNECTION_POOLING	1	enabling or disabling *connection pooling* (a cache of database connections at the database-end that can be reused when the database receives future requests for data) to RiskFort Server.
MAX_ACTIVE	128	Total number of active connections from the pool. 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 C-11 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.
TRANSPORT_TYPE	TCP	Default value for RiskFort Server to start up is TCP. Set this parameter to **TLS**, if RiskFort Native protocol is set to TLS. In other words, set this parameter to TLS, if you want to enable TLS-based secure communication between Administration Console and WebFort Server. **NOTE:** You *must* restart RiskFort Server, if you change the value to TLS.

Table C-11 Parameters for Communication Between Risk Evaluation Java SDK and RiskFort Server

Parameter	Default	Description
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: The parameters in the file are separated by a semicolon (;).

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.properties**, the values that you specify in this file can differ. You might need to do so to accomodate the time lag that occurs in Issuance-related operations.

Refer to Table C-11 for more information on configuration parameters in this file.

log4j.properties.riskfort_sdk

The log4j.properties.riskfort_sdk file specifies the logging behavior of RiskFort and its Risk Evaluation components.

The following table provides information to configure `log4j.properties.riskfort_sdk` file.

Table C-12 Parameters for log4j.properties Configuration

Parameter	Description
`log4j.appender.debuglog.File`	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.Max-FileSize`	The maximum allowed file size of the log file. The default value is set to `10MB`.
`log4j.appender.debuglog.Max-BackupIndex`	The index number to create the instance of the log file, if the log file is full.

log4j.properties.riskfort_issuance

The `log4j.properties.riskfort_issuance` file specifies the logging behavior of RiskFort and its Issuance components. The following table provides information to configure `log4j.properties.riskfort_issuance` file.

Table C-13 Parameters for log4j.properties Configuration

Parameter	Description
`log4j.appender.debuglog.File`	The name of the log file. Possible values for this parameter are: • `arissuancews.log` -> for Issuance Web `Service` • `arcotissuance.log` -> for Issuance Java SDK
`log4j.appender.debuglog.Max-FileSize`	The maximum allowed file size of the log file. The default value is set to `10MB`.
`log4j.appender.debuglog.Max-BackupIndex`	The index number to create the instance of the log file, if the log file is full.

NOTE: The **`log4j.properties.issuance`** file in the `<install_location>/arcot/sdk/java/properties` has been deprecated and *should not* be used, unless you are using older Issuance APIs.

Sample Configuration Files

This section provides the content of the default configuration files that appear after installation. It covers the following:

- **arcotcommon.ini**
- **riskfortserver.ini**
- **adminserver.ini**
- **regfort.ini**
- **jni.ini**
- **riskfort.properties.***
- **log4j.properties**

arcotcommon.ini

The default content of the `arcotcommon.ini` file is as follows:

```
#---------------------------------------------------------------#
#            Arcot Database configuration
#---------------------------------------------------------------#

#---------------------------------------------------------------#
#    Note: The "Default" value defines the value that will be
#    used if either the parameter is not present or its value
#    has not been provided.
#---------------------------------------------------------------#

#---------------------------------------------------------------#
#    Note: All of these configurations can be overridden in the
#    server's ini file at a section level. Please refer to the
#    manuals for more details.
#---------------------------------------------------------------#

#---------------------------------------------------------------#
#   This section covers the global configurations for database
#   connectivity

##DbType:
#   The type of the database applicable to all database  conns.
```

```
#    Allowed values are: oracle, mssqlserver.
#    Default: oracle

##Driver:
#    This indicates the fully-qualified name of the database
#    driver class that is supplied by the jdbc driver vendor.
#   Consult your jdbc vendor documentation for the right driver
#    name.
#    For Oracle: oracle.jdbc.driver.OracleDriver
#   For SQLServer: com.microsoft.sqlserver.jdbc.SQLServerDriver
#    Default: No internal default, must be set

##MaxConnections:
#    This indicates the maximum number of database connections
#    that the server can keep at any point in time. This could
#    have impact on the number of concurrent database queries
#    that server can process.
#    Default: 32.

##MinConnections:
#    This indicates the minimum number of database connections
#    that server should keep.
#    Default: 16.

##IncConnections:
#   This indicates the number by which the database connections
#   is to be incremented till the number of connections reaches
#    MaxConnections.
#    Default: 4.

##AutoRevert:
#    This flag indicates whether the server needs to check if
#    any of the primary databases are up again (to switch back
#    to) when all the primary databases have gone down (and the
#    server has switched to the backup databases).
#    Default: 1.

##MaxTries:
#    This indicates the maximum number of attempts to make to
#    connect to the database.
#    Default: 3.

##ConnRetrySleepTime:
#    This indicates the time in *milli seconds* to sleep before
#    making another attempt to connect to the database.
#    Default: 100.
```

```
##MonitorSleepTime:
#    This indicates the amount of time in *seconds* the
#    Monitoring Thread sleeps between heartbeat checks on all
#    the databases.
#    Default: 50.

##Profiling:
#    This flag indicates whether detailed database connection
#    information needs to be logged. Allowed values are: 0
#    (Off), 1 (On).
#    Default: 0.

##EnableBrandLicensing:
#    This indicates whether branded ODBC driver license is
#    enabled or not. Allowed values are: 0 (Off), 1 (On).
#    Default: 0.

##BrandLicenseFile:
#    This indicates the branded ODBC driver license file path
#    relative to ODBC_HOME.
#    This is required if EnableLicensing=1. Otherwise this is
#    ignored.

##MaxTransactionRetries:
#    This indicates the maximum number of time the transaction
#    will be retried on the same database instance for certain
#    error conditions.
#    Default: 3.

##TransactionRetrySleepTime:
#    This indicates the time gap between transaction retries in
#    *milliseconds*.
#    Default: 10 milliseconds.
#-------------------------------------------------------------#
[arcot/db/dbconfig]

DbType=
Driver=
MaxConnections=
MinConnections=
IncConnections=
AutoRevert=
MaxTries=
ConnRetrySleepTime=
MonitorSleepTime=
Profiling=
EnableBrandLicensing=
```

```
BrandLicenseFile=
MaxTransactionRetries=
TransactionRetrySleepTime=

#-------------------------------------------------------------#
#   This section covers the configuration for the primary
#    database connectivity

##Datasource:
#    The name of the data source as defined in ODBC.

##URL:
#    The name of the JDBC data source.
#    Oracle- jdbc:oracle:thin:@<server>:<port>:<sid>
#    SQLServer-
#jdbc:sqlserver://<server>:<port>;databaseName=<databasename>;
#selectMethod=cursor

##Username:
#    The username corresponding to Datasource.<N>.
#    The password corresponding to Username.<N> needs to be
#    securely stored in MasterHSMDevice with value of
#    Datasource.<N> as the key.
#   The dbutil utility is used to achieve this. Please read the
#    supplied manuals for dbutil.

#-------------------------------------------------------------#
[arcot/db/primarydb]

Datasource.1=
URL.1=
Username.1=

#-------------------------------------------------------------#
#   This section covers the configuration for the backup
#    database connectivity

##Datasource:
#    The name of the data source as defined in ODBC.

##URL:
#    The name of the JDBC data source.
#    Oracle- jdbc:oracle:thin:@<server>:<port>:<sid>
#    SQLServer-
#jdbc:sqlserver://<server>:<port>;databaseName=<databasename>;
#selectMethod=cursor
```

```
##Username:
#    The username corresponding to Datasource.<N>.
#    The password corresponding to Username.<N> needs to be
#    securely stored in MasterHSMDevice with value of
#    Datasource.<N> as the key.
#   The dbutil utility is used to achieve this. Please read the
#    supplied manuals for dbutil.

#-------------------------------------------------------------#
[arcot/db/backupdb]

#Datasource.1=
#URL.1=
#Username.1=

#-------------------------------------------------------------#
#   This section covers the configuration for instance-wide
#   parameters

##InstanceId:
#    This identifies this specific installation instance (for
#    all servers) in a multi-instance deployment.
#    It is highly recommended that this is set to an unique
#    value for each deployment instance.
#    Default: 1.

#-------------------------------------------------------------#
[arcot/system]

InstanceId=

#-------------------------------------------------------------#
#    This section covers the configuration for HSM device
#    information

##MasterHSMDevice:
#    This specifies the name of the HSM device where the
#    MasterKey is present. The MasterKey is typically used to
#    encrypt data like database passwords and so on.
#    Default: The protected data is in securestore.enc.

##MasterHSMDevicePinLocation:
#    The location from where the MasterHSMDevice pin is to be
#    obtained. Allowed values are:
#    FILE  - Pin is to be obtained from securestore.enc with
#            valueOf(MasterHSMDevice) as the key.
#   PROMPT- Pin is to be obtained from a client after server is
```

```
#            partially-started up.
#    This parameter has no meaning if the MasterHSMDevice is
#    configured as empty.
#    Default: FILE.

#-------------------------------------------------------------#
[arcot/crypto/device]

MasterHSMDevice=
MasterHSMDevicePinLocation=

#-------------------------------------------------------------#
#    This section covers the configuration for watchdog process
#    that monitors Arcot servers.
#    Note: This section is applicable only for UNIX platform(s).

##ServerStartsTimeout:
#    watchdog will stop restarting the server if the server
#    restarts [ServerStartsCount] times in
#    [ServerStartsTimeout]. This parameter is in *minutes*.
#    Default: 25.

##ServerStartsCount:
#    This is the number of times the server sleep time in *milli
#    seconds* after which the watchdog restarts the server once
#    the server has gone down.
#    Default: 5.

##RestartSleepTime:
#    This is the sleep time in *milli seconds* after which the
#    watchdog restarts the server once the server has gone down
#    Default: 5000.
#-------------------------------------------------------------#
[arcot/watchdog]

ServerStartsTimeout=
ServerStartsCount=
RestartSleepTime=
```

riskfortserver.ini

The default content of the `riskfortserver.ini` file is as follows:

```
#-------------------------------------------------------------#
#             Arcot RiskFort Server configuration
#-------------------------------------------------------------#
#-------------------------------------------------------------#
#  Note: The "Default" value defines the value that will be   #
#  used if either the parameter is not present or its value   #
#  has not been provided.                                     #
#-------------------------------------------------------------#

#-------------------------------------------------------------#
#    Configuration for the log file
[arcot/riskfort/logger]

#    This is the location of the text file where RiskFort will
#    log.
#    The path can be an absolute path or relative to ARCOT_HOME.
#    Default: logs/arcotriskfort.log.
LogFile=logs/arcotriskfort.log

#    The size in *bytes* of each log file after which a new one
#    would be created. The current one is moved to
#    BackupLogFileDir.
#    Default: 10485760
LogFileSize=10485760

#    This is the location of the directory where backup of the
log #    file is to be created after the current one exceeds
#    LogFileSize bytes.
#    Default: logs/backup.
BackupLogFileDir=logs/backup

#    This is the initial logging level applicable unless an
#    override is specified through an ArAdmin request.
#    Allowed values are: 0 (FATAL), 1 (WARNING), 2 (INFO), 3
#    (DETAIL).
#    Default: 1.
LogLevel=1

#    This indicates whether the time zone information logged in
#    the logfile is in GMT or local time.
#    Allowed values are: 0 (local time), 1 (GMT).
#    Default: 0.
LogTimeGMT=0
```

```
#-------------------------------------------------------------#

#-------------------------------------------------------------#
#    Configuration for server parameters
[arcot/riskfort/server]

#    This indicates the maximum number of threads that server
#    can keep at any point in time. This has a direct impact of
#    the number of concurrent requests server can process.
#    Default: 128.
MaxThreads=128

#    This indicates the minimum number of threads that server
should keep.
#    should keep.
#    Default: 32.
MinThreads=32
```

adminserver.ini

The default content of the `adminserver.ini` file is as follows:

```
#-------------------------------------------------------------#
#             Arcot Admin Console configuration
#-------------------------------------------------------------#
#-------------------------------------------------------------#
#  Note: The "Default" value defines the value that will be   #
#  used if either the parameter is not present or its value   #
#  has not been provided.                                     #
#-------------------------------------------------------------#

#-------------------------------------------------------------#

#    WebFort Connection related configuration
##transport
#   WebFort transport mechanism. Permitted values are TCP and
#    TLS
#    Default:TCP

##server.CACert
#    Complete path of the Trusted Root Certificate for TLS
#    connection with WebFort
#    Default: <empty>

##remotehost.1:
#    Webfort host information
```

```
#    Default:localhost

##remoteport.1:
#    Webfort port information
#    Default:9742

#-------------------------------------------------------------#
[arcot/admin/authconfig]
remotehost.1=
remoteport.1=
transport=
server.CACert=
#-------------------------------------------------------------#
#    This section has other configurations required for ADMIN
#    Console application

##serverInfo:
#    Reports needs this.
#    Default:localhost:80

##JNILibraryPath:
#    This specifies the path in file system where the JNI
libraries delivered with
#    Arcot application is present.
#    Default: No default

#-------------------------------------------------------------#
[arcot/admin/config]
serverInfo=localhost:80
#JNILibraryPath=<ABSOLUTE_JNI_DIR_PATH>
[arcot/admin/manager]
```

regfort.ini

```
#-------------------------------------------------------------#
#               Arcot Issuance Configuration
#-------------------------------------------------------------#
#-------------------------------------------------------------#
#  Note: The "Default" value defines the value that will be   #
#  used if either the parameter is not present or its value   #
#  has not been provided.                                     #
#-------------------------------------------------------------#

#-------------------------------------------------------------#

[arcot/regfort/config]
```

```
#    This specifies the path in file system where the JNI
#    libraries delivered with Arcot application is present.
#    Default: No default
JNI_LIBRARY_PATH=<ABSOLUTE_JNI_DIR_PATH>
```

jni.ini

```
#-----------------------------------------------------------------#
#                  Arcot JNI configuration
#-----------------------------------------------------------------#
#-----------------------------------------------------------------#
#  Note: The "Default" value defines the value that will be   #
#  used if either the parameter is not present or its value   #
#  has not been provided.                                      #
#-----------------------------------------------------------------#

#-----------------------------------------------------------------#
#    Configuration for the log file
[arcot/jni/logger]

#    This is the location of the text file where WebFort will
#    log.
#    The path can be an absolute path or relative to ARCOT_HOME.
#    Default: logs/arcotjni.log.
LogFile=logs/arcotjni.log

#    The size in *bytes* of each log file after which a new one
#    would be created. The current one is moved to
#    BackupLogFileDir.
#    Default: 10485760
LogFileSize=10485760

#    This is the location of the directory where backup of the
log #   file is to be created after the current one exceeds
#    LogFileSize bytes.
#    Default: logs/backup.
BackupLogFileDir=logs/backup

#    This is the initial logging level applicable unless an
#    override is specified through an ArAdmin request.
#   Allowed values are: 0 (FATAL), 1 (WARNING), 2 (INFO), 3
#    (DETAIL).
#    Default: 1.
LogLevel=1
```

```
#    This is to turn on/off the creation of the JNI log file.
#    Default: 1.
CreateLog=1
#-------------------------------------------------------------#

#-------------------------------------------------------------#
# Configuration for OpenSSL CA
[arcot/jni/opensslca]

#    This is the location of the configuration file used by
#    OpenSSL. The path can be an absolute path or relative to
#    ARCOT_HOME.
#    Default: tools/opensslca/ca.cnf
ConfigFile=tools/opensslca/ca.cnf

#    This is the location of file which contains the CA's
#    private key. The path can be an absolute path or relative
#    to ARCOT_HOME.
#    Default: The corresponding parameter present in ConfigFile
#    is attempted. If it is not available in ConfigFile, it
#    further defaults to: tools/opensslca/private/cakey.pem.
PrivateKeyFile=tools/opensslca/private/cakey.pem

#    This is the location of the CA certificate file
#    corresponding to the private key.
#    The path can be an absolute path or relative to ARCOT_HOME.
#    Default: The corresponding parameter present in ConfigFile
#    is attempted.
#    If it is not available in ConfigFile, it further
#    defaults to:tools/opensslca/cacert.pem.
CACertFile=tools/opensslca/cacert.pem

#    This indicates whether the textual data (CN, DN etc.) in
#    the certificate is represented as UTF-8 or ASCII.
#    Allowed values are: 0 (Off), 1 (On).
#    Default: 0.
UseUTF8=0
#-------------------------------------------------------------#

#-------------------------------------------------------------#
#    Configuration for reusable key pair
[arcot/jni/keyring]

#    This represents the key size of the reusable
#    key-certificate pair used for ArcotID generation for
#    improved performance.
#    Default: A new key-certificate pair will be generated for
```

```
#    each ArcotID.
PlainKeyBitSize=1024
#-------------------------------------------------------------#

#-------------------------------------------------------------#
#    Configuration for Admin requests
[arcot/jni/admin]

#    This is the location of the directory where the domain and
RA
#    certificates generated by the CA are stored.
#    The path can be an absolute path or relative to ARCOT_HOME.
#    Default: certs/certificates.
CertDirectory=certs/certificates

#    This is the location where the RA's private key and
#    certificate is stored when Admin requests RA store
#    creation. This is also used byRegfort to obtain the
#    location of the RA store.
RAStore=certs/p12stores/rastore.p12

#   This is the location where the domain's key and certificate
#    are stored when Admin requests domain key/certificate
#    creation.
DomainStore=certs/p12stores/domainkeystore.p12
#-------------------------------------------------------------#
```

riskfort.properties.*

```
#-------------------------------------------------------------#
#    RiskFort server IP address
HOST.1=localhost

#    RiskFort server port number
PORT.1=7680

#    Parameter name for connection timeout with RiskFort Server
CONNECTION_TIMEOUT=30000

#    Parameter name for connection retries with RiskFort Server
CONNECTION_RETRIES=3

#    Parameter name for read timeout on a connection with
#    RiskFort Server.
READ_TIMEOUT=30000
```

```
#    Parameter for enabling or disabling the connection pooling
     to RiskFort Server. Default is enabled, set
     USE_CONNECTION_POOLING=0 for disabling connection pooling.
USE_CONNECTION_POOLING=1

#    Parameter name for maximum number of active connections
#    with RiskFort Server this client will manage.
MAX_ACTIVE=128

#    Ensure that TIME_BETWEEN_CONNECTION_EVICTION +
     IDLE_TIME_OF_CONNECTION < firewall connection timeout.
#    Example: If your firewall times out and closes idle
     connections in 1 hour, #then you can set
     IDLE_TIME_OF_CONNECTION to 1800000 milliseconds(30 mins)
#   and the Evictor Thread to run after 900000 milliseconds (15
minutes)

#    Time(in milliseconds) between connection evictor thread
     runs. Comment it out to prevent the closing of idle
     connections by RiskFort SDK.
TIME_BETWEEN_CONNECTION_EVICTION=900000

#    Idle time(in milliseconds) of connections after which they
     should be closed.
IDLE_TIME_OF_CONNECTION=1800000

#    Parameter name for behavior of client when all connections
#    are exhausted.
WHEN_EXHAUSTED_ACTION=BLOCK

#    Transfort Type, Possible values are TCP and TLS
TRANSPORT_TYPE=TCP

#     Required if TRANSPORT_TYPE = TLS: CA certificate file.
CA_CERT_FILE=<server CA certificate (in PEM format) file path>

#-----------------------------------------------------------------#
```

log4j.properties

```
#-----------------------------------------------------------------#
log4j.rootLogger=WARN, debuglog
log4j.logger.com.arcot=WARN
log4j.logger.com.arcot.database=WARN
log4j.logger.com.arcot.cache=WARN
log4j.logger.com.arcot.service=WARN
```

```
log4j.logger.org.hibernate=WARN

log4j.appender.debuglog=org.apache.log4j.RollingFileAppender
log4j.appender.debuglog.File=<Filename.log>

log4j.appender.debuglog.MaxFileSize=10MB
# Keep one backup file
log4j.appender.debuglog.MaxBackupIndex=200

log4j.appender.debuglog.layout=org.apache.log4j.PatternLayout
log4j.appender.debuglog.layout.ConversionPattern=%d [%t] %-5p
%-5c{3}(%L) %x -> %m%n

#-------------------------------------------------------------#
```

Appendix D

Database Reference

RiskFort database contains a number of tables, some of which grow with increased usage of the product. This appendix describes the tables in RiskFort that grow. 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 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 how to calculate the database size while you are planning to set up the database for RiskFort. This appendix also lists all tables used by RiskFort and trimming some recommendations.

- **Database Sizing Calculations**
- **RiskFort Database Tables and Truncation Recommendations**

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 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 transactions per day (**T**) = 24,000
- Number of entries in the Quova Data Feed (**Q**) = 10,000,000 (ten million)
- Computation tomfooleries (**D**) = 90 days

Sample Calculations Based on Assumptions Made

Considering the figures assumed in section, **"Value Assumptions Made,"** the final requirement should be:

- Based on **total number of users**, the database size = (5 * *N*) KB
- Based on **daily activity,** the database size = (*T* * *D* * 5) KB
- Based on the **size of Quova Data Feed,** the database size = (*Q* * 2) KB

RiskFort Database Tables and Truncation Recommendations

Table D-1 lists all RiskFort database tables and their description.

Table D-1 RiskFort Tables

Table Name	Description
ARSERVERS	Stores Arcot product component registrations.
ARLOCALE	Stores the localization information.
ARCONFIG	Stores global RiskFort configuration information.
ARCLIENTSSLROOTCAS	Stores path to the client Root CA certificate for two-way SSL authentication.
ARPROTOCOLREGISTRY	Stores listener port information.
ARGROUP	Stores fixed configuration information for groups.
ARSUBGROUP	Stores fixed configuration information for subgroups.
ARGROUPCONFIG	Stores configuration information for groups.
ARSUBGROUPCONFIG	Stores configuration information for subgroups.
ARUSER	Stores user attributes.
ARTXID	Stores the unique Transaction ID for each instance.
ARSERVERREGISTRY	Stores the information related to all instances of all components.
ARRESOURCECATEGORY	Stores information about DB Resource Types for all products.
ARACTIONCONSTANTS	Stores
ARPOLICIES	Stores information about the levels of administrators supported.
ARPRIVILEGE	Stores information about privileges available to each administrator level.
ARADMIN	Stores information about all existing administrators in the system.
ARADMINDOMAIN	Stores information about the GROUP(s) administered by an administrator.
ARADMINAUDITLOG	Stores activity logs for administrator actions.

Table D-1 RiskFort Tables

Table Name	Description
ARCACHEREFRESH	Stores the information required for communicating cache-refresh event across multiple instances of Administration Console.
ARRFADVICECODE	Stores configuration information for risk advice.
ARRFCREDENTIAL	Stores configuration information for supported credentials. **Note:** This table is currently not used.
ARRFACTION	Stores configuration information for all supported user actions.
ARRFADVICECONFIG	Stores configuration information for score and advice mapping at group level.
ARRFSYSRULESETS	Stores the configuration information for rulesets at group level. **Note:** This table stores both history and the changes made by the administrator.
ARRFCURRENTRULESET	Stores the currently used configuration of rulesets at group level.
ARRFSYSRULES	Stores the configuration information for all rules and rulesets. This information includes version and configuration for each rule. **Note:** This table stores both history and the changes made by the administrator.
ARRFTRUSTEDIPLIST	Stores the list of all trusted aggregators.
ARRFUNTRUSTEDIPLIST	Stores the list of all negative IP addresses.
ARRFSYSAUDITLOG	Stores all logs related to risk evaluation and other activity audits.
ARRFDEVICEINFO	Stores the 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.
ARRFEXCEPTIONUSER	Stores the list of users marked as exception users.
ARRFEXCPUSERHIST	Stores the history of all users who were marked as exception users.

Table D-1 RiskFort Tables

Table Name	Description
ARRFSYSTERMINATINGRULES	Stores configuration information for each rule and the corresponding result that impacts the risk score.
ARRFSYSSCOREMATRIX	Stores all rules and corresponding results that impact the risk score.
ARRFNEGATIVECOUNTRYLIST	Stores the list of all negative countries.
ARQGeoPoint1	Stores the geo-location information for different ranges of IP addresses. This information is obtained from Quova.
ARQGeoPoint2	Stores the geo-location information for different ranges of IP addresses. This information is obtained from Quova.
ARCREDLOG	Stores audit information for the following Issuance activities: • Create • Reissue/reset • Delete
ARADMINAUDITLOG	Stores activity logs for administrator actions.

Tables That Can be Truncated

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.

- **ARRFDEVICEINFOHIST**

  This table stores the history of a Device. By deleting entries here, you will reduce the amount of analysis that can be performed on how users access from various devices or how devices vary over time for the same user.

- **ARCREDLOG**

  This table contains the information of the actions that are performed on the credentials. By deleting entries from this table, the amount of available reporting data is reduced.

- **ARADMINAUDITLOG**

This table contains the history of all actions performed by administrators.

ARUSER

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 delete user data in the ARUSER table. For example, you might want to delete 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 ARUSER 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.

Tables That Can Not be Truncated

The tables discussed in this section are used for risk scoring and grow based on the usage. As a result, it is highly recommended that you do not trim these tables. These tables are:

- **ARRFDEVICEINFO**

  RiskFort Server makes an entry every time it receives a request from a new device. It issues each new device a unique DEVICEID and stores the information to identify the device for subsequent logins. The table also contains last-observed information about the device. This table grows when a new device is detected or when the device information changes.

- **ARRFDEVUSERASSO**

  This table identifies an association between a device and the corresponding user. This table grows when a user logs in from a new device. The device can be relative to the user and earlier might have been used by a different user. The entries in this table are made or updated if the application calling RiskFort chose to associate a name/tag with the user device. An association between a user and device will exist only if the user has successfully completed the second authentication.

Appendix E

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

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.

The following table lists the default port numbers used by RiskFort.

Table E-1 Default Port Numbers

Protocol Module	Default Port Number	Description
RiskFort Native	7680	The RiskFort Native protocol is a proprietary binary protocol supported by RiskFort. Applications integrating with RiskFort must use this protocol to communicate with the RiskFort Server.
Server Management	7980	This protocol is used for the management of RiskFort Server. **Note:** Currently, the protocol only supports server cache refresh and shut-down requests.
Issuance	7690	This protocol is used by RiskFort Server for issuance-related activities, such as creating or updating users in RiskFort database.

If you do not want to use the default port numbers, then you can specify a different set of port numbers by editing the `riskfortserver.ini` file.

On Linux platform, `riskfortserver.ini` is available at the following location:

`<install_location>/arcot/conf/riskfortserver.ini`

URLs for RiskFort Components

Use the URLs listed in the following table to access RiskFort components after installation. The URLs in the table use the default ports.

Table E-2 Default Port Numbers

Component or Service	URL
Administration Console	http://<*hostname*>:<*port*>/arcotadmin/adminlogin.htm
Issuance Web Service	http://<*hostname*>:<*port*>/arcotriskfortissuancews/services/ArcotRiskFortIssuanceWebService
Sample Application	http://<*hostname*>:<*port*>/riskfort-1.7-sample-application/index.jsp
Risk Evaluation Web Service	http://<*hostname*>:<*port*>/arcotriskfortws/services/RiskFortXActionService
Issuance WSDL File	http://<*hostname*>:<*port*>/arcotriskfortissuancews/services/ArcotRiskFortIssuanceWebService.wsdl
Risk Evaluation WSDL File	http://<*hostname*>:<*port*>/arcotriskfortws/services/RiskFortXActionService

Appendix F

Third-Party Software Used

This appendix lists the third-party software packages that are used by RiskFort. These include:

ANTLR 2

Copyright © 2003-2006, Terence Parr. Public-domain software.

Apache

Copyright The Apache Software Foundation. Licensed under the Apache License, Version 2.0.

- `log4j` (Copyright © 1999-2007 The Apache Software Foundation)
- `Axis2` (Copyright © 2000-2005 The Apache Software Foundation)
- `Apache Commons` (Copyright © 2001-2008 The Apache Software Foundation)
  - `commons-beanutils`
  - `commons-collections`
  - `commons-digester`
  - `commons-fileupload`
  - `commons-lang`
  - `commons-logging`
  - `commons-pool`
  - `commons-validator`
- `struts` (Copyright © 2000-2007 The Apache Software Foundation)
- `jakarta-oro` (Copyright © 1994-2004 The Apache Software Foundation)

Bouncy Castle

Cryptix

dom4j

Hibernate Core 3.1

JSON

OpenSSL

Oracle Database 10*g* JDBC Driver

Spring Framework

Sun Microsystems

- Java Mail (Copyright © 1994-2008 Sun Microsystems, Inc.)
- JSTL (Copyright © 1994-2008 Sun Microsystems, Inc.)

Appendix G

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.
Authentication Token	A token is an object that an authorized user of computer services is given to aid in authentication.
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 Rule**s 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, WebFort Server, 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. This protocol is predecessor of Transport Layer Security (TLS).
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.
Transport Layer Security (TLS)	Protocol to secure and authenticate communications across public networks by using data encryption.
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