Arcot RiskFort™
Quick Installation Guide
(for Unix Platforms)
Version 2.2.6

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot RiskFort Quick Installation Guide
Version 2.2.6
October 2010
Part Number: RF-0226-QIGU-10

Trademarks

Patents

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

Third Party Software

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

This Quick Installation Guide covers:

1. Checking System Requirements
2. Installing RiskFort
3. Performing Post-Installation Tasks
4. What's Next?

Checking System Requirements

The computer where you plan to install all or any components of RiskFort must meet the hardware and software requirements listed in this section.

Hardware Requirements

The minimum hardware requirements for RiskFort are:

- **RAM:** 1 GB
- **Hard Disk:** 10 GB
- **Processor:** 2.4 GHz

Software Requirements

The minimum software requirement for RiskFort are:

- **Operating System:**
  - Solaris SPARC 10
  - Red Hat Enterprise Linux 4.0 and 5.0
- **Service Pack:** SP2 or higher
- **Database Server:**
  - Oracle 10*g* or higher
- **Directory Server:**
  - SunOne Directory Server 5.2
  - SunOne Directory Server 6.1
- **Application Server:**
  - Apache Tomcat 5.5.23 or higher
  - IBM WebSphere 6.1 or higher
  - BEA WebLogic 10 or higher

NOTE: Use JDK version that is best compatible with the Application Server that you are using.

Installing RiskFort

You can install RiskFort on a single system, or you can distribute its components on more than one system.

For instance, if you would like to distribute RiskFort components on two systems, then typically you will install the Server, Administration Console, and UDS component on one system, while the Java SDKs and Sample Application can be installed on the second system.

NOTE: If you plan to perform distributed installation, then you must run the installer individually on all target systems and select the required components to install.

To install RiskFort.

1. Run the installation wizard.:
   - **For Solaris:** `Arcot-RiskFort-2.2.6--Solaris-Installer.bin`.
   - **For Linux:** `Arcot-RiskFort-2.2.6--Linux-Installer.bin`.
2. Follow the instructions on the screen.
3. On the Installation Type screen:
   - Select **Complete** if you want to install all RiskFort components on one system.
   - Select **Custom** if you want to distribute RiskFort components on different systems, and then select the required components on the Component Selection screen.
4. Complete the installation by following the on-screen instructions.

IMPORTANT: Ensure that you restart the system before you proceed with Performing Post-Installation Tasks.

Performing Post-Installation Tasks

This section guides you through:

1. Running Database Scripts
2. Verifying the Database Setup
3. Deploying Web Applications

4. Logging Into and Bootstrapping the Administration Console
5. Starting RiskFort Server
6. Starting the Case Management Queuing Server
7. Verifying the Installation
8. Deploying and Using the Sample Application

IMPORTANT: If you performed a two-system distributed installation, as discussed in section "Installing RiskFort", then you must perform Steps **1** through **6** on the first system and only Step **7** on the second system.

Running Database Scripts

To seed the RiskFort database schema:

1. Navigate to the appropriate database directory (`oracle`) in:

   `<install_location>/arcot/dbscripts/`

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

   - `arcot-db-config-for-common-1.0.sql`
   - `arcot-db-config-for-riskfort-2.2.6.sql`

Verifying the Database Setup

To verify if the RiskFort database was set up correctly:

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

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

   You must see the following output:

   ```
   SERVERNAME   VERSION

   ----------------------   ------

   RiskFort                 2.2.6

   RiskFortCaseManagement   2.2.6
   ```

3. Log out of the database console.

Deploying Web Applications

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

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

The important steps to deploy these applications include:

1. Preparing Your Application Server
2. Deploying UDS and Verifying the Deployment
3. Deploying Administration Console and Verifying the Deployment

Preparing Your Application Server

On Apache Tomcat:

To copy the Arcot-proprietary files on Apache Tomcat:

1. Copy `ArcotAccessKeyProvider.so` to:
   - **For Solaris:** `$JAVA_HOME/jre/sparc/`
   - **For RHEL:** `$JAVA_HOME/jre/bin/`
2. Copy `arcot-crypto-util.jar` to `$JAVA_HOME/jre/lib/ext/`.
3. Restart the application server.

On IBM WebSphere

To copy the Arcot-proprietary files:

1. Log into WebSphere Administration Console.
2. Click **Environment**, and then click **Shared Libraries**.
   a. From the **Scope** drop-down, select a valid visibility scope. The scope must include the target server or node on which the application is deployed.
   b. Click **New**.
   c. Enter the **Name**, for example, *ArcotJNI*.
   d. Specify the **Classpath**. (This path must point to the location where `arcot-crypto-util.jar` is present and must also include the file name. For example, `/opt/arcot/ext/arcot-crypto-util.jar`.)

e. Enter the **JNI Library** path. (This path must point to the location where `ArcotAccessKeyProvider.so` is present.)

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

On BEA WebLogic

To copy the Arcot-proprietary files on WebLogic server:

1. Copy `ArcotAccessKeyProvider.so` to:
   - **For Solaris:** `$JAVA_HOME/jre/sparc/`
   - **For RHEL:** `$JAVA_HOME/jre/bin/`
2. Copy `arcot-crypto-util.jar` to `$JAVA_HOME/jre/lib/ext/`.

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

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

Deploying UDS and Verifying the Deployment

To deploy the UDS WAR file on your application server:

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

   `<install_location>/arcot/java/webapps/`

NOTE: The deployment procedure depends on the application server that you are using. Refer to your application server vendor documentation for detailed instructions.

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

      `<install_location>/arcot/logs/`

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

These lines indicate that UDS was deployed successfully. You might also want to make sure that the log file does not contain any `FATAL` and `WARNING` messages.

Deploying Administration Console and Verifying the Deployment

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

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

   `<install_location>/arcot/java/webapps/`

NOTE: The deployment procedure depends on the application server that you are using. Refer to your application server vendor documentation for detailed instructions.

2. Restart the application server.
3. To verify if the console started correctly:
   a. Navigate to the following location:

   `<install_location>/arcot/logs/`

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

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

These lines indicate that the console was deployed successfully. You might also want to make sure that the log file does not contain any `FATAL` and `WARNING` messages.

Logging Into and Bootstrapping the Administration Console

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

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

   Here, *host* and *port* must be for the application server where you deployed the Console.
2. Log in by using the default MA credentials:
   - User Name: **masteradmin**
   - Password: **master1234!**
3. Click **Begin** to start the bootstarpping process.
4. Specify the **Old Password**, **New Password**, **Confirm Password**, and click **Next**.
5. Specify the UDS configuration parameters. You can accept the defaults.
6. Specify the **Display Name** and **Authentication Mechanism** for the Default Organization, and click **Next**.
7. Click **Continue** to complete the bootstrapping process.

Starting RiskFort Server

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`
2. Run the `./riskfortserver start` command.

Starting the Case Management Queuing Server

To start the Case Management Queuing Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`
2. Run the `./casemanagementserver start` command.

Verifying the Installation

To verify the installation:

1. Navigate to the following location:

   `<install_location>/arcot/logs/`
2. Open `arcotriskfort.log` in any editor and locate the following lines:
   - `STARTING Arcot RiskFort 2.2.6_s`
   - `STARTING Arcot RiskFort 2.2.6_l`
   - `Arcot RiskFort Service READY.`

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

Deploying and Using the Sample Application

To deploy the Sample Application:

1. Stop the application server services.
2. Deploy riskfort-2.2.6-sample-application.war from the following location:

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

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

3. Access the Sample Application by specifying the URL:

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

4. (***For distributed installation only***) Configure the Sample Application to communicate with RiskFort Server:

   a. Open the riskfort.risk-evaluation.properties file in an editor window. This file is available at:

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

   b. Set the value for following parameters:

   - HOST.1
   - PORT.1

5. Restart the application server.
6. Follow the instructions on the screen to:

   a. Perform risk evaluation for a user who has not been created in the RiskFort database.

   b. Create the user in the RiskFort database.

   c. Perform risk evaluation again for the same user.

What's Next?

After completing the post-installation tasks, you must then configure the Java Application Programming Interfaces (APIs) and Web services provided by RiskFort.

- Configuring Risk Evaluation Java SDK
- Configuring Issuance Java SDK
- Configuring Web Services

Configuring Risk Evaluation Java SDK

To configure the RiskFort Risk Evaluation SDK:

1. From ARCOT_HOME/sdk/java/**lib**/, copy the JAR files to the appropriate location on your <APP_SERVER_HOME> directory. (For example, on Apache Tomcat this location is <*APP_HOME*>/WEB-INF/**lib**/.)

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

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

   - If your application already has a configured log4j file, then merge it with the following files:
     - <*install_location*>/arcot/sdk/java/properties/log4j.properties.risk-evaluation
     - <*install_location*>/arcot/sdk/java/properties/riskfort.risk-evaluation.properties
   - If the application does not have the log4j file already configured, then:

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

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

iii. Copy the log4j.properties file to <*APP_HOME*>/WEB-INF/classes/**properties**/.

Configuring Issuance Java SDK

To configure RiskFort Issuance SDK:

1. From ARCOT_HOME/sdk/java/**lib**/, copy the JAR files to the appropriate location on your <*APP_SERVER_HOME*> directory. (For example, on Apache Tomcat this location is <*APP_HOME*>/WEB-INF/**lib**/.)
   - /arcot/arcot_core.jar
   - /arcot/arcot-riskfort-issuance.jar
   - /arcot/arcot-pool.jar
   - /external/bcprov-jdk14-139.jar
   - /external/commons-beanutils-1.7.0.jar
   - /external/commons-collections-3.1.jar
   - /external/commons-lang-2.0.jar
   - /external/commons-logging-1.0.4.jar
   - /external/commons-pool-1.4.jar
   - /external/dom4j-1.6.1.jar
   - /external/jaxen-1.1-beta-8.jar
   - /external/jdom-1.0.jar
   - /external/log4j-1.2.9.jar
   - /external/oro-2.0.8.jar
   - /external/xalan-2.7.0.jar
   - /external/xercesImpl-2.6.2.jar
   - /external/xml-apis-1.0.b2.jar
   - /external/xmlParserAPIs-2.6.2.jar
   - /external/xom-1.1.jar
2. Configure the log4j.properties.riskfort-issuance and riskfort.issuance.properties files:
   - If your application already has a configured log4j file, then merge it with the following files:
     - <*install_location*>/arcot/sdk/java/properties/log4j.properties.riskfort-issuance
     - <*install_location*>/arcot/sdk/java/properties/riskfort.issuance.properties
   - If the application does not have the log4j.properties file already configured, then:
     i. Rename log4j.properties.riskfort-issuance to log4j.properties.
     ii. Merge riskfort.issuance.properties with log4j.properties.
     iii. Copy the log4j.properties file to <*APP_HOME*>/WEB-INF/classes/**properties**/.

Configuring Web Services

If you are using RiskFort Web services, then:

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

   <*install_location*>/arcot/wsdls/**riskfort**/
3. Generate the respective client code by using the following WSDLs:
   - **ArcotRiskFortEvaluateRiskSvc.wsdl**: For Risk Evaluation Web Service.
   - **ArcotRiskFortIssuanceSvc.wsdl**: For Issuance Web Service.
4. Restart the application server.
5. In a browser window, access the following URLs to verify if the client can access the Web Service:
   - **Risk Evaluation:**

     http://<RISKFORT_SERVER_IP>:<PORT>/services/RiskFortEvaluateRiskSvc
   - **Issuance:**

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