

# **Arcot WebFort®**

## **Quick Installation Guide**

**(for Unix Platforms)**

**Version 6.2**



**455 West Maude Avenue, Sunnyvale, CA 94085**

Arcot WebFort Quick Installation Guide  
Version 6.2  
May 2010  
Part Number: WF-0062-0QIG-10

Copyright © 2010 Arcot Systems, Inc. All rights reserved.

This guide, as well as the software described herein, is furnished under license and may be used or copied only in accordance with the terms of the license. The content of this guide is furnished for informational purposes only. It is subject to change without notice and should not be construed as a commitment by Arcot Systems.

Arcot Systems makes no warranty of any kind with regard to this guide. This includes, but is not limited to the implied warranties of merchantability, fitness for a particular purpose or non-infringement. Arcot Systems shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Except as permitted by the software license, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior written permission of Arcot Systems, Inc.

## **Trademarks**

Arcot®, ArcotID®, WebFort, and WebFort VAS® are registered trademarks of Arcot Systems, Inc. The Arcot logo™, the Authentication Authority tagline, ArcotID Client™, ArcotOTP™, RegFort™, RiskFort™, SignFort™, TransFort™, and Arcot Adapter™ are all trademarks of Arcot Systems, Inc.

All other product or company names may be trademarks of their respective owners.

## **Patents**

This software is protected by United States Patent No. 6,170,058, 6,209,102 and other patents pending.

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

## **Third Party Software**

All the third-party software used by WebFort and related components are listed in the appendix “Third-Party Software Licenses” of *Arcot WebFort 6.2 Installation and Deployment Guide*.

This Quick Installation Guide covers:

1. [Checking System Requirements](#)
2. [Installing WebFort](#)
3. [Performing Post-Installation Tasks](#)
4. [What's Next?](#)

## Checking System Requirements

---

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

### Hardware Requirements

The minimum hardware requirements for WebFort are:

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

### Software Requirements

The minimum software requirement for WebFort are:

- **Operating System:** Solaris 10 (SPARC), Red Hat Enterprise Linux 4.0 (x86), or Red Hat Enterprise Linux 5.0 (x86)
- **Service Pack:** Latest
- **Database Server:**
  - Oracle 10g or 11g
  - IBM DB2 9.5
- **Directory Server:**
  - SunOne Directory Server 5.2
  - SunOne Directory Server 6.1
- **Application Server:**
  - Apache Tomcat 5.5.23
  - IBM WebSphere 6.1
  - BEA WebLogic 10

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

## Installing WebFort

---

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

For instance, if you would like to distribute WebFort 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 WebFort.

1. Run the installation wizard by clicking `Arcot-WebFort-6.2-<platform name>-Installer.bin`.
2. Follow the instructions on the screen.
3. On the Installation Type screen:
  - Select **Complete** if you want to install all WebFort components on one system.
  - Select **Custom** if you want to distribute WebFort 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 WebFort Server](#)

- 6. [Verifying the Installation](#)
- 7. [Deploying and Using the Sample Application](#)

**IMPORTANT:** If you performed a two-system distributed installation, as discussed in section “Installing WebFort”, then you must perform [Step 1](#) through [Step 6](#) on the first system and only [Step 7](#) on the second system.

## Running Database Scripts

To seed the WebFort database schema:

1. Navigate to the appropriate database directory ([oracle](#) or [db2](#)) in:  
  
`<install_location>/arcot/dbscripts/`
2. Run the scripts in the *following* order:
  - [arcot-db-config-common-1.0.sql](#)
  - [arcot-db-config-for-webfort-6.2.sql](#)

## Verifying the Database Setup

To verify if the WebFort database was set up correctly:

1. Log in to the WebFort 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
-----	-----
WebFort	6.2

3. Log out of the database console.

## Deploying Web Applications

User Data Service (UDS) and Administration Console are Web-based WebFort 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 [libArcotAccessKeyProvider.so](#) to  
`%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.)
  - e. Enter the **JNI Library** path. (This path must point to the location where [libArcotAccessKeyProvider.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 `libArcotAccessKeyProvider.so` to `<JAVA_HOME_WebSphere>/jre/bin/`.
  6. Restart WebSphere.

## On BEA WebLogic

To copy the Arcot-proprietary files on WebLogic server:

1. Copy `libArcotAccessKeyProvider.so` to WebLogic's `<JAVA_HOME_WebLogic>/jre/bin/`.
2. Copy `arcot-crypto-util.jar` to WebLogic's `<JAVA_HOME_WebLogic>/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:
    - UDS Initialized successfully
    - Starting Arcot User Data Service (Version: 1.0.8)

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 `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. 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 v1.0.8
  - 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 bootstrapping 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 WebFort Server

To start the WebFort Server:

1. Navigate to the following directory:

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

2. Run the following command:

```
./webfortserver start
```

## Verifying the Installation

To verify the installation:

1. Navigate to the following location:

```
<install_location>/arcot/logs/
```
2. Open `arcotwebfortstartup.log` in any editor and locate the following lines:
  - INSTANCE\_VER.....: [6.2]
  - Arcot WebFort Authentication 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. Navigate to **Settings, Control Panel, Administrative Tools, Services**.
2. Stop the application server services.
3. Deploy `webfort-6.2-sample-application.war` from the following location:

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

**NOTE:** Although you will also see `webfort-6.2-sample-application.war` in the package, it is recommended that you deploy the Sample Application file from the preceding location only.
4. Access the Sample Application by specifying the URL:

```
http://<host>:<port>/webfort-6.2-sample-application/
```
5. (*For distributed installation only*) Configure the Sample Application to communicate with WebFort Server:
  - a. Click the **Setup -> Server Connectivity** link.
  - b. Set the value for following parameters:
    - IP Address
    - Port
  - c. Click **Set Up** to save the connection.

6. Restart the application server.
7. Follow the instructions on the screen to:
  - a. Create the user in the WebFort database.
  - b. Create credentials for the user.
  - c. Perform authentication

## What's Next?

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

- [Configuring Authentication Java SDK](#)
- [Configuring Issuance Java SDK](#)
- [Configuring Web Services](#)

## Configuring Authentication Java SDK

To configure the WebFort Authentication Java SDK:

1. From `<install_location>/arcot/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-pool.jar`
  - `arcot/arcot-webfort-common.jar`
  - `arcot/arcot-webfort-authentication.jar`
  - `external/bcprov-jdk14-139.jar`
  - `external/commons-httpclient-3.1.jar`
  - `external/commons-lang-2.4.jar`
  - `external/commons-pool-1.4.jar`
  - `external/log4j-1.2.9.jar`
2. Edit the `<install_location>/arcot/sdk/java/properties/webfort.authentication.properties` file to set the following:
  - `authentication.host.1`: Host name or IP address of WebFort Server.
  - `authentication.port.1`: Port number configured for the Authentication Native protocol. The default value is 9742.

## Configuring Issuance Java SDK

To configure WebFort Issuance Java SDK:

1. From `<install_location>/arcot/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-pool.jar`
  - `arcot/arcot-webfort-common.jar`
  - `arcot/arcot-webfort-issuance.jar`
  - `external/activation-1.1.jar`
  - `external/axiom-api-1.2.7.jar`
  - `external/axiom-impl-1.2.7.jar`
  - `external/axis2-adb-1.4.jar`
  - `external/axis2-java2wsdl-1.4.jar`
  - `external/axis2-kernel-1.4.jar`
  - `external/backport-util-concurrent-2.2.jar`
  - `external/bcprov-jdk14-139.jar`
  - `external/commons-codec-1.3.jar`
  - `external/commons-collections-3.1.jar`
  - `external/commons-httpclient-3.1.jar`
  - `external/commons-lang-2.4.jar`
  - `external/commons-logging-1.1.jar`
  - `external/commons-pool-1.4.jar`
  - `external/geronimo-jms_1.1_spec-1.1.jar`
  - `external/log4j-1.2.9.jar`
  - `external/neethi-2.0.jar`
  - `external/stax-api-1.0.1.jar`
  - `external/wsdl4j-1.6.2.jar`
  - `external/wstx-asl-3.2.0.jar`
  - `external/XmlSchema-1.2.jar`
2. Configure the `<install_location>/arcot/sdk/java/properties/webfort.issuance.properties` file to set the following:
  - `issuance.host.1`: Host name or IP address of WebFort Server.
  - `issuance.port.1`: Port number configured for the Transaction Web Services protocol. The default value is 9744.

## Configuring Web Services

If you are using WebFort Web services, then:

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

```
<install_location>/arcot/wsdl/webfort/
```

3. Generate the respective client code by using the following WSDLs:
  - [ArcotWebFortAuthSvc.wsdl](#): For Authentication Web Service.
  - [ArcotWebFortIssuanceSvc.wsdl](#): For Issuance Web Service.
4. Restart the application server.