Arcot WebFort® Installation and Deployment Guide (for Solaris)

Version 5.4.1

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot WebFort Installation and Deployment Guide
Version 5.4.1
June 2008
Part Number: AWF01-002DC-05410

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".

Contents

Preface **5**
Purpose of this Guide 5
Intended Audience 5
Information Included in this Guide 5
Related Publications 6
Conventions Used in This Book 7

Chapter 1 Understanding WebFort **9**
Product Description 10
What is New in This Release 11

Chapter 2 Planning the Deployment **13**
Deployment Overview 14
Choosing a Deployment Model 16
Deploying on a Single System 16
Component Diagrams 17
Deploying on Distributed Systems 19
Component Diagrams 19
Architecture Diagram 21
Deploying for High Availability 22
Component Diagrams 22
Architecture Diagram 23
Deploying WebFort Basic 23

Chapter 3 Preparing for Installation **25**
System Requirements 26
Hardware Requirements 26

Software Requirements 26
Prerequisite Software for WebFort Components 26
Minimum Software Requirements 27
Location for Downloading Prerequisite Software 29
Configuring Database Server 31
Configuring Oracle Database 31
Getting Ready for Installation 33
Database Requirements 33
Requirements for Java-Dependant Components 34

Chapter 4 Deploying WebFort on a Single System 35
Installing WebFort 37
Post-Installation Tasks 41
Running Database Scripts 41
Testing the Installation 42
Starting WebFort Server 42
Stopping WebFort Server 42
Verifying the Log Files 43
Configuring OpenSSLCA 43
Deploying Administration Console 45
Logging In to Administration Console 45
Creating a Domain Key 46
Creating a Global Administrator 47
Configuring TLS Communication (Optional) 48
Between WebFort Server and Administration Console 48
Between WebFort Server and Authentication SDK 50
Between WebFort Server and Authentication Web Service 50
Deploying Sample Application 50
Configuring Sample Application for WebFort Server 51
Using Sample Application 51
Creating User and ArcotID 51
Downloading ArcotID 52
Authenticating using ArcotID 52

Chapter 5 Deploying WebFort on Distributed Systems 55
Installing on First System 57
Post-Installation Tasks for First System 61
Running Database Scripts 61
Testing the Installation 62
Starting WebFort Server 62
Stopping WebFort Server 62
Verifying the Log Files 63

Configuring OpenSSLCA 63
Deploying Administration Console 65
Logging In to Administration Console 65
Creating a Domain Key 66
Creating a Global Administrator 67
Configuring TLS Communication (Optional) 68
Between WebFort Server and Administration Console 68
Installing on Second System 70
Post-Installation Tasks for Second System 71
Copying the Configuration Files 71
Configuring TLS Communication (Optional) 71
Between WebFort Server and Authentication SDK 71
Between WebFort Server and Authentication Web Service 71
Working with Sample Application 72
Deploying Sample Application 72
Configuring Sample Application for WebFort Server 73
Using Sample Application 73

Chapter 6 Performing Basic Installation 75
Installing WebFort 76
Post-Installation Tasks 78
Testing the Installation 78
Starting WebFort Server 78
Stopping WebFort Server 78
Verifying the Log Files 79
Configuring TLS Communication (Optional) 79

Chapter 7 Configuring APIs and Web Services 83
Introduction to WebFort APIs 84
Authentication API 84
Issuance API 84
Configuring Java APIs 85
Configuring Authentication Java APIs 85
Configuring Issuance Java APIs 86
Configuring Web Services 88
Configuring Authentication Web Services 88
Configuring Issuance Web Services 89

Chapter 8 Uninstalling WebFort 91
Removing the Database 92
Uninstalling WebFort 93
Post-Uninstallation Steps 94

Appendix A WebFort File System Structure 95
WebFort File Structure 96

Appendix B Configuration Files and Options 99
INI Files 100
arcotcommon.ini 100
Database Settings 100
LDAP Settings 103
Instance Settings 105
webfortserver.ini 105
Log File Settings 106
Thread Settings 107
adminserver.ini 108
Authentication Settings 108
regfort.ini 109
jni.ini 109
Log File Settings 110
Configurations for OpenSSL CA 111
Configuring Reusable Key Pair 112
Configuration for Administration Console 112
Properties Files 114
authenticator.properties 114
log4j.properties 115

Appendix C Database Reference 117
Database Sizing Calculations 118
Denotations Used in Sample Calculations 118
Value Assumptions Made 118
Sample Calculation Based on Assumptions Made 118
Database Tables and Truncating Recommendations 119
Tables That can be Truncated 121

Appendix D Default Port Numbers and URLs 123
Default Port Numbers 124
URLs for WebFort Components 125

Appendix E Third-Party Software Licenses 127

Appendix F Glossary 129

Index 133

Preface

The Arcot WebFort 5.4.1 Installation and Deployment Guide provides information for planning and deploying WebFort, based on different solution requirements. Each solution consists of multiple components that interact with each other and other systems in an enterprise or multiple-network systems.

Purpose of this Guide

This section describes the intended audience for this guide, contents of the guide, publications related to the guide, and the conventions used across the guide.

Intended Audience

This guide is intended for architects, system administrator, database administrators, system integrators, Web developers, and others who are responsible for the installation, deployment, and maintenance of Arcot WebFort.

> **NOTE:** Some tasks in this guide are intended for users who are comfortable with SQL database administration tasks, like creating databases and users, installing database drivers, and running SQL scripts. If you are not familiar with these tasks, Arcot recommends that you have an experienced database administrator perform them.

Information Included in this Guide

This guide is organized as follows:

- **Chapter 1, "Understanding WebFort"** describes the features and architecture of WebFort.
- **Chapter 2, "Planning the Deployment"** describes the different deployment options and the architecture details related to each deployment.
- **Chapter 3, "Preparing for Installation"** discusses the requirements for installing WebFort. It also provides configuration and planning-related information.
- **Chapter 4, "Deploying WebFort on a Single System",** lists the installation and post-installation tasks for single-system deployment.
- **Chapter 5, "Deploying WebFort on Distributed Systems",** lists the installation and post-installation tasks for distributed-system or high-availability deployment.
- **Chapter 6, "Performing Basic Installation"**, lists the installation and post-installation tasks for Basic deployment.
- **Chapter 7, "Configuring APIs and Web Services"** describes the steps to configure the APIs and Web services provided by WebFort.
- **Chapter 8, "Uninstalling WebFort"** guides you through the steps for uninstalling WebFort components.
- **Appendix A, "WebFort File System Structure"** provides the information about the location of all the files that are installed by the WebFort installer.
- **Appendix B, "Configuration Files and Options"** discusses the configuration files that WebFort uses and the parameters that you must configure in these files.
- **Appendix C, "Database Reference"** discusses the fast-growing WebFort tables and their trimming recommendations.
- **Appendix D, "Default Port Numbers and URLs"** lists the default port numbers and URLs that WebFort uses.
- **Appendix E, "Third-Party Software Licenses"** lists the license text of third-party software packages that are used by WebFort.
- **Appendix F, "Glossary"** lists the key terms related to WebFort.

Related Publications

Other related publications are as follows:

Arcot WebFort 5.4.1 Administration Guide	This guide includes the information to administer and configure WebFort.

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Enter **Y** to agree the license agreement.
Italic	Key Words	First time log in to the *Administrative Console* must be done using Master Admin credentials.
	Names of Publications	For more information, see the *Arcot WebFort 5.4.1 Administration Guide*.
	Emphasis	*Never* give anyone your password.
Cross reference	Links in the guide	Refer to the section **Upgrading WebFort** for more information.
`Fixed-width`	Command-line input or output	`# cd /opt/arcot`
	Code Samples	`var walletname = "GuestUser";`

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

	File names	`arcotcommon.ini`

Chapter 1

Understanding WebFort

This chapter introduces you to WebFort and discusses the following topics:

- Product Description
- What is New in This Release

Product Description

Arcot WebFort is an authentication server that provides software-only, two-factor authentication to protect and verify the identity of the users. WebFort upgrades security from simple user name/password authentication without changing the user login experience or critical business processes by using an ArcotID for authentication.

The ArcotID is a secure software credential that does not require any software to be installed on an user's computer to provide two-factor authentication. With zero installed client software, the ArcotID can be used from any computer.

ArcotID can be typically used for adding strong authentication to Web applications, Virtual Private Networks (VPNs), intra-enterprise usage, and other solutions like secure signing, bill payments and so on.

Based on Arcot's patented *Cryptographic Camouflage*™ technology, ArcotID is *not* vulnerable to brute-force, Man-in-the-Middle (MITM), and other attacks that can be mounted against other software tokens. While, based on PKI technology, ArcotID Web authentication does not require the deployment of any PKI infrastructure.

WebFort also supports authentication through basic user name/password, Question and Answers (Q&A), and One Time Passwords (OTP).

In addition to being an authentication mechanism, ArcotID can also act as a secure container for digital IDs (also know as email certificates or signing certificates) in place of expensive Smart Cards or USB security tokens. Users with Digital IDs can be enabled to digitally sign common file formats (PDFs, email, MS Word) and to safely receive PKI encrypted files, such as a billing statement or purchase order through email.

What is New in This Release

The following are the new features and enhancements provided by WebFort 5.4.1:

1. Support to use email address as user name.
2. The WebFort 5.4.1 version extends support to authenticate users from external directories using LDAP. If WebFort is configured for LDAP authentication, then the users in the *Administrator* group are authenticated using user name/password authentication and users in other groups, will use the LDAP authentication.

Chapter 2

Planning the Deployment

The following deployment-related topics are covered in this chapter:

- Deployment Overview
- Choosing a Deployment Model

Deployment Overview

This section briefs the tasks for deploying WebFort so that it can issue ArcotID secure software credential and then authenticate users.

Perform the following steps to deploy WebFort:

1. Choose a deployment model that suits your business needs, see "Choosing a Deployment Model".
2. Install all prerequisite software, see "System Requirements" for more information on the prerequisite software.
3. Set up a new database user in the database server, see "Configuring Database Server" fore more information on configuring the database.
4. Install WebFort components, refer to the following sections:
   - "Deploying WebFort on a Single System" for Complete installation.
   - "Deploying WebFort on Distributed Systems" for Custom installation.
   - "Performing Basic Installation" for Basic installation.
5. Run SQL scripts in the database to create the Arcot schema and set initial configuration values. Refer to the following:
   - "Running Database Scripts" for single-system deployment.
   - "Running Database Scripts" for distributed-system deployment.
6. Deploy and start the Web-based Administration Console. Refer to the following:
   - "Deploying Administration Console" for single-system deployment.
   - "Deploying Administration Console" for distributed-system deployment.
7. Log in to Administration Console and create a domain key to enable ArcotID issuance and authentication. Refer to the following:
   - "Logging In to Administration Console" for single-system deployment.
   - "Logging In to Administration Console" for distributed-system deployment.
8. Create a Global Administrator user for setting additional configuration values. Refer to the following:
   - "Creating a Global Administrator" for single-system deployment.
   - "Creating a Global Administrator" for distributed-system deployment.

9. Deploy Sample Application to test the WebFort installation. Refer to the following:
   - "Deploying Sample Application" for single-system deployment.
   - "Deploying Sample Application" for distributed-system deployment.

   NOTE: The tasks you perform while installing WebFort depends on the deployment model you select.

Choosing a Deployment Model

This section helps you to select a deployment model and determine the WebFort components and prerequisite software that you must install on each system. Architecture diagrams for deployment models are also provided to assist you with planning.

WebFort Server is the primary component for installation. It validates authentication requests from Web applications, VPNs, or software using ArcotID authentication.

Apart from WebFort Server, Java SDKs and Web Services are provided for issuing ArcotIDs to users and authenticating the users. Your Web applications can use these components to integrate with WebFort Server.

WebFort requires a SQL database for storing server configuration data, user-specific preferences, and audit log data.

WebFort also provides a Sample Application, which can be used to verify if WebFort is installed successfully, able to issue ArcotIDs, and authenticate users. Sample Application also serves as a code sample for integrating WebFort with your existing Web applications.

Typically, the WebFort components and Web applications for ArcotID issuance and authentication are installed on a single system for development and simple testing. In production deployments and staging environments, WebFort Server and Web applications must be on separate systems, and SDKs on the system that contains the Web applications.

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

The following deployment models are discussed in this chapter:

- **Deploying on a Single System**
- **Deploying on Distributed Systems**
- **Deploying for High Availability**
- **Deploying WebFort Basic**

Deploying on a Single System

In a single-system deployment, all the components of WebFort and the Web applications that users log in to are installed on a single system. The database can be on the same system where WebFort 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, refer to "Software Requirements" for the prerequisite software for these components.

To deploy WebFort on a single system, you must choose the *Complete* option during WebFort installation. See Chapter 4, "Deploying WebFort on a Single System" for more information on the installation and post-installation steps.

Component Diagrams

The component diagrams depict few of the possible deployment options for prerequisite software and WebFort components. If you perform a Complete install, then both Java SDKs and Web Services will be installed on the system. You can use any of these methods for integrating WebFort with your Web application.

- Deploying Using Java SDKs
- Deploying Using 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 WebFort 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 recommends to build your own Web application using Sample Application as a code-reference.

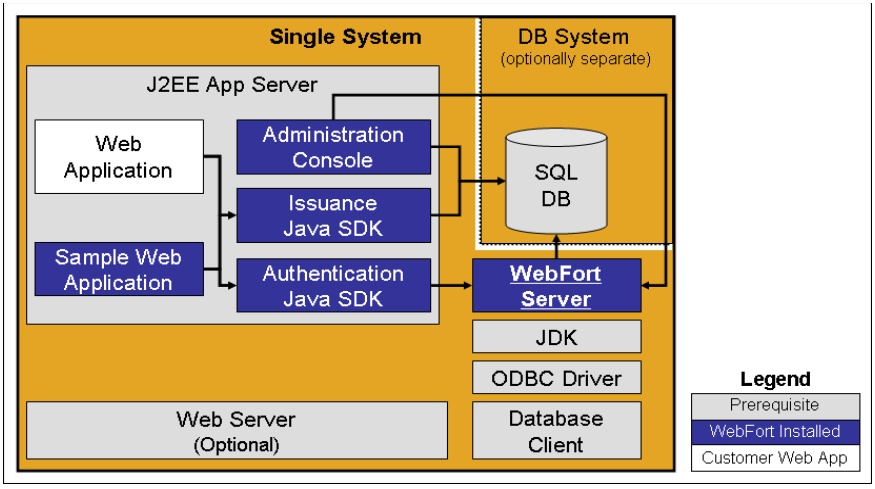
Decision: Use Java SDKs or Web Services to integrate with your own Web application.

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

Deploying Using Java SDKs

The following figure illustrates deployment of WebFort Server and Java SDKs on a single system.

Figure 2-1

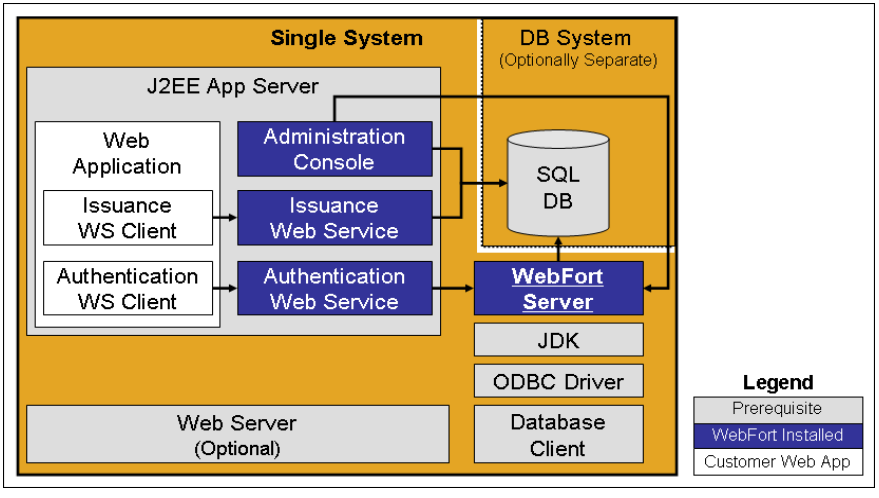


NOTE: The use of a Web server to deliver HTML pages for the J2EE application server is optional and transparent to WebFort. In production deployments, it is generally used to improve application server performance and security. Refer to the documentation of your application server for further information.

Deploying Using Web Services

The following figure illustrates deployment of WebFort Server and Web Services on a single system.

Figure 2-2



Deploying on Distributed Systems

In a distributed-system deployment, WebFort components are installed on different systems. This type of deployment increases the security, performance, and enables multiple applications to use ArcotID strong authentication. This model is typically used for production deployments or staging environments.

The most common deployment is to install WebFort Server on one system and one or more Web applications on additional systems. To deploy WebFort on distributed systems, you must choose the *Custom* option during WebFort installation. See **Chapter 5, "Deploying WebFort on Distributed Systems"** for more information on the installation and post-installation steps.

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

- **Component Diagrams**
- **Architecture Diagram**

Component Diagrams

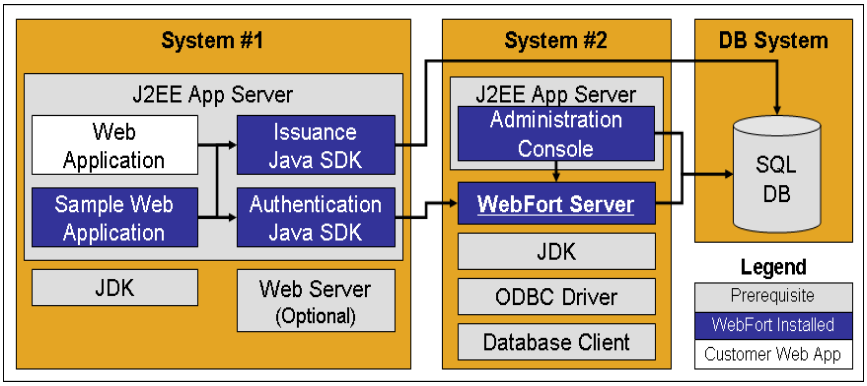
The following diagrams depict which prerequisite software and WebFort components can be installed on each system for a distributed-system deployment:

- **Deploying Java SDKs on a Single Application**
- **Deploying Java SDKs on Multiple Applications**
- **Deploying Web Services on a Single Application**

Deploying Java SDKs on a Single Application

The following figure illustrates deployment of WebFort using Java SDKs on a single application.

Figure 2-3

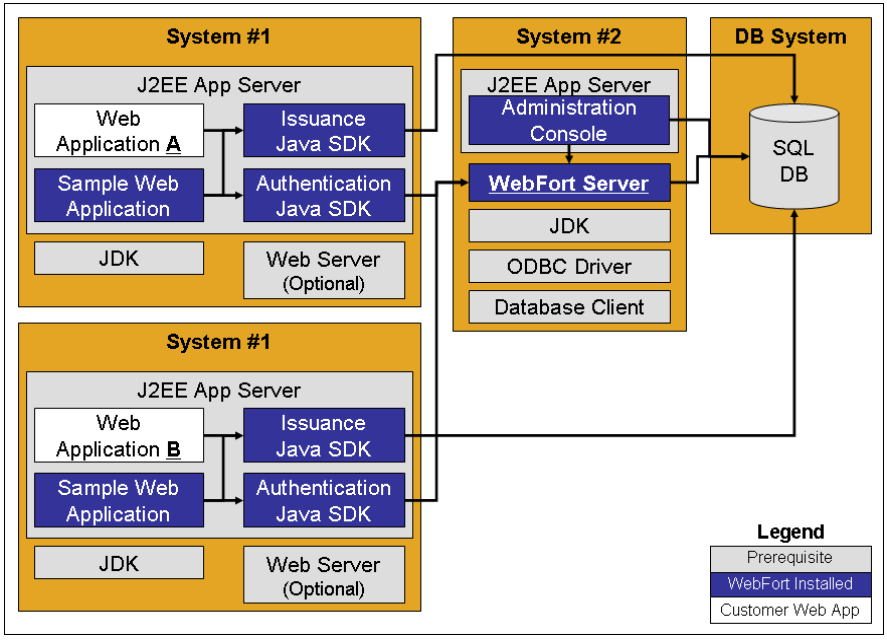


NOTE: Administration Console can be installed on any or all the systems.

Deploying Java SDKs on Multiple Applications

The following figure illustrates deployment of WebFort using Java SDK on multiple applications.

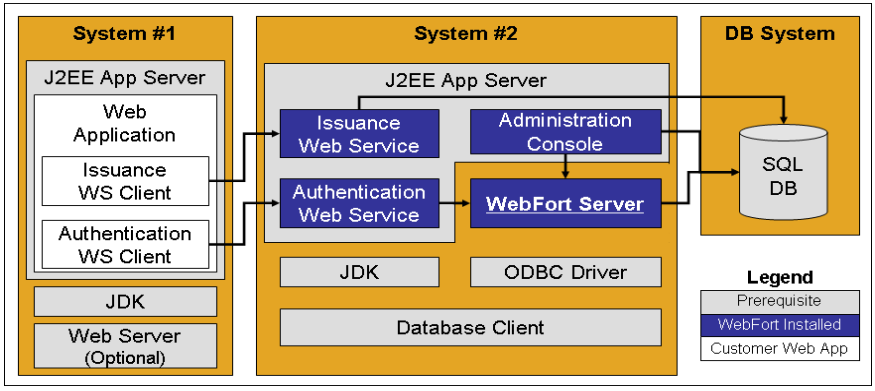
Figure 2-4



Deploying Web Services on a Single Application

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

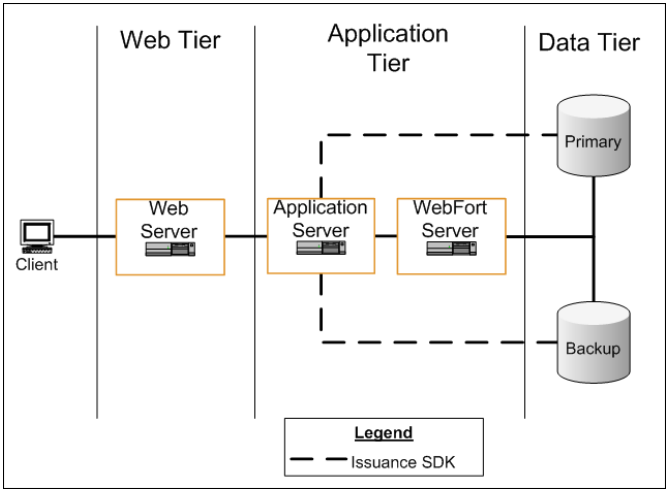
Figure 2-5



Architecture Diagram

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

Figure 2-6



NOTE: Load balancers can be used appropriately based on network architecture.

Deploying for High Availability

In a high-availability deployment, WebFort is installed on more than one server to ensure operational continuity.

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

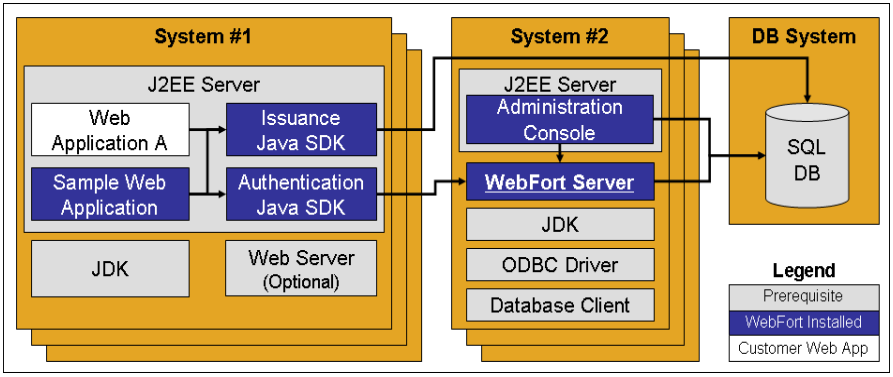
- Component Diagrams
- Architecture Diagram

Component Diagrams

Deploying for High Availability Using Java SDKs

The following figure illustrates multiple instances of WebFort components using Java SDK.

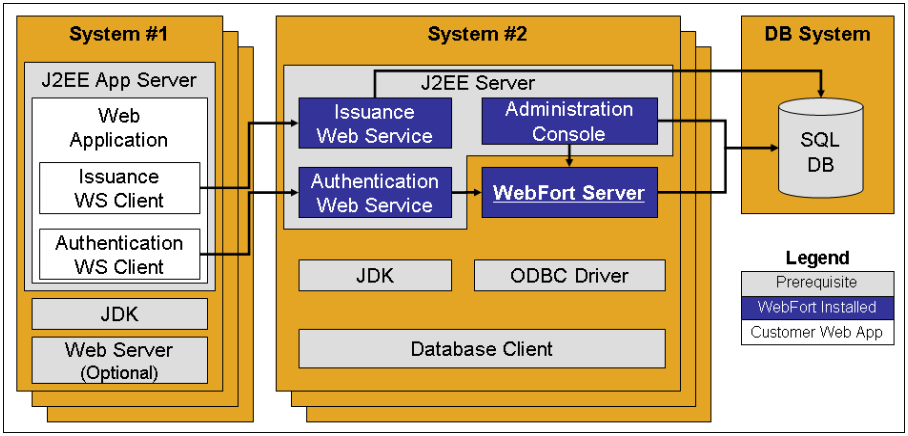
Figure 2-7



Deploying for High Availability Using Web Services

The following figure illustrates multiple instances of WebFort components using Web Services.

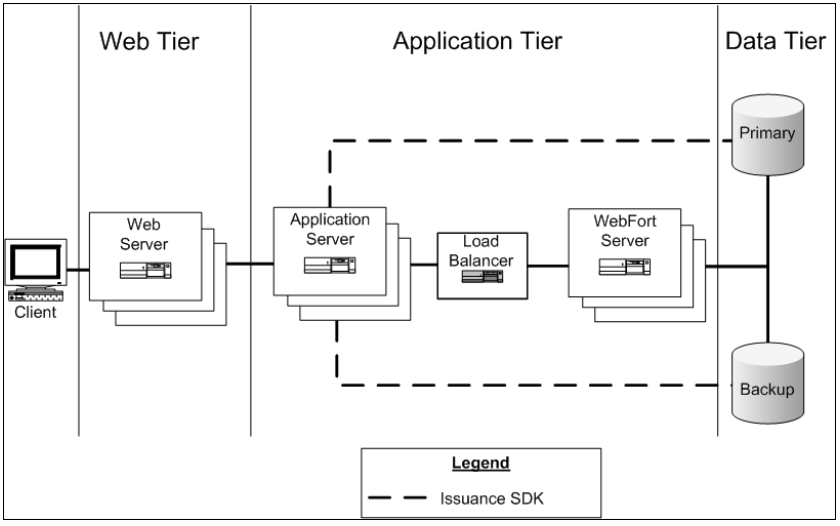
Figure 2-8



Architecture Diagram

The following figure shows the architecture diagram for a high-availability deployment.

Figure 2-9



Deploying WebFort Basic

In the Basic deployment only WebFort Server is installed. This type of deployment is required to provide WebFort functionality to other Arcot products.

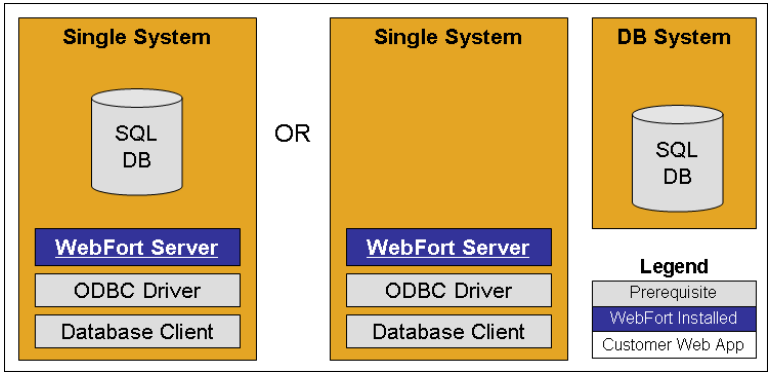
The Arcot Administration Console is a common component included in many Arcot products. It uses WebFort Server to authenticate administrators during login, therefore WebFort is a prerequisite component for other products.

Other Arcot products also include a limited license to use some features of WebFort.

To perform the basic installation of WebFort, you must choose the *Basic* option during WebFort installation. See **Chapter 6, "Performing Basic Installation"** for more information on the installation and post-installation steps.

The following figure illustrates the basic deployment of WebFort.

Figure 2-10



Chapter 3

Preparing for Installation

Before installing WebFort, ensure that your computer meets the requirements described in this chapter. The chapter also provides configuration and planning-related information. It contains the following sections:

- System Requirements
- Configuring Database Server
- Getting Ready for Installation

System Requirements

This section lists the minimum software and hardware requirements to install WebFort:

- Hardware Requirements
- Software Requirements

Hardware Requirements

The following values specify the hardware required for WebFort (only) and does not include the hardware that is required for the prerequisite software. The following values can be used when deploying WebFort for development purposes:

1. Requirements for WebFort with database on same system:
   - RAM: 512 MB
   - Hard Drive Space: 10 GB
2. Requirements for WebFort with database on a different system:
   - RAM: 256 MB
   - Hard Drive Space: 300 MB

Software Requirements

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

- Prerequisite Software for WebFort Components
- Minimum Software Requirements
- Location for Downloading Prerequisite Software

Prerequisite Software for WebFort Components

The prerequisite software required by WebFort is determined by the WebFort components that are installed on a system. Refer to Chapter 2, "Planning the Deployment" to determine which WebFort components to install for a specific deployment type.

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

Table 3-1 Prerequisite Software for WebFort Components

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

Minimum Software Requirements

This section lists the supported software list for the following versions of Solaris operating system:

- Solaris 9
- Solaris 10

Solaris 9

This section lists the following software requirements that your computer must meet for installing WebFort successfully:

- Database Requirements
- JDK and Application Server Requirements

Database Requirements

Table 3-2 provides all the supported software required for the Database that is used by WebFort for Solaris 9. See Table 3-3 for the corresponding versions of supported JDK and application server.

Table 3-2 Database Requirements for Solaris 9

Supported Platform	Database Server	Database Client	ODBC Driver
Solaris 9	Oracle 9i	Oracle 9.0.2	Arcot Branded DataDirect ODBC Driver 05.20.0048 (Oracle Client Protocol)

JDK and Application Server Requirements

Table 3-3 provides the version of JDK and application server supported by WebFort for Solaris 9.

Table 3-3 JDK and Application Server Requirements for Solaris 9

Supported Platform	Sun JDK	Application Server
Solaris 9	1.4.2_13	Tomcat 5.0.28

Solaris 10

This section lists the following software requirements that your computer must meet for installing WebFort successfully:

- Database Requirements
- JDK and Application Server Requirements

Database Requirements

Table 3-4 provides all the supported software required for creating the Database that is used by WebFort for Solaris 10. Refer to Table 3-5 for the corresponding version of supported JDK and Application server.

Table 3-4 Database Requirements for Solaris 10

Supported Platform	Database Server	Database Client	ODBC Driver
Solaris 10	Oracle 10g	Oracle 10g	Arcot-branded DataDirect ODBC Driver 05.20.0048 (Oracle Client Protocol)
	Oracle 9i	Oracle 9.0.2	Arcot-branded DataDirect ODBC Driver 05.20.0048 (Oracle Client Protocol)

JDK and Application Server Requirements

Table 3-5 provides the version of JDK and Application server supported by WebFort for Solaris 10.

Table 3-5 JDK and Application Server Requirements for Solaris 10

Supported Platform	Sun JDK	Application Server
Solaris 10	5.0 Update 10	Tomcat 5.5.23
	1.4.2_13	Tomcat 5.0.28

NOTE: *Sun JDK 1.5* and *Sun JDK 5.0* are equivalent terms.

Location for Downloading Prerequisite Software

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

1. **Sun JDK Archive Downloads (for both 1.4 & 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. **Sun JDK 1.4.2**

   http://java.sun.com/j2se/1.4.2/download.html

4. **Tomcat 5.5.23** (`5.5.23.sh`)

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

5. **Tomcat 5.0.28** (`5.0.28.sh`)

   http://archive.apache.org/dist/tomcat/tomcat-5/v5.0.28/bin/

Configuring Database Server

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

WebFort supports a primary and a backup database that is used during failover and failback in a high-availability deployment. Database connectivity can be configured during WebFort installation or by manually editing the **arcotcommon.ini** file.

WebFort can use an already existing database, but for security reasons it is recommended that you create a new database, which is used only by Arcot servers.

> **NOTE:** To protect the database, Arcot strongly recommends that the database server is protected with firewalls or other access control mechanisms.

> **IMPORTANT:** The system which has the database server and the system which has the Arcot products ***must*** have the same time-zone setting.

Configuring Oracle Database

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

Running WebFort 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 must be a separate tablespace.

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

NOTE: Refer to Oracle database documentation to perform the tasks listed in this sub-section.

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 WebFort 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 - 10GB for a development or test deployment, which is primarily used for audit logs.

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

3. Grant the user with CONNECT and RESOURCE privileges.
4. Grant the user with CREATE TABLESPACE privilege.

Getting Ready for Installation

Perform the following tasks described in this section on the system where you will install WebFort or which uses WebFort components:

- Database Requirements
- Requirements for Java-Dependant Components

Database Requirements

The following steps will help you to complete the Oracle database setup:

1. Get the following database information from the DBA:

   a. **TNS Service Name** - Use of *arcotdbtns* is recommended

   b. **User Name** - Login

   c. **Password**

   d. **Service ID** - The Service ID of the database created.

   e. **Port Number**

   f. **Host name**

   Refer to Table 4-2 for more information on these parameters.

2. Install Oracle Client

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

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

3. TNS Names Setup

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

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

4. Install the Arcot-branded ODBC Driver

Based on the entry for WebFort Database in the tnsnames.ora file, you must edit the `odbc.ini` file to create a new DSN for WebFort Database. Ensure that the DSN uses the supported ODBC driver mentioned in the "Software Requirements" section.

> **NOTE:** You must set up the database before you start the WebFort installation. Also, to set up the database, you need superuser (root) privileges.

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

a. Log in to the Solaris OS.

b. Navigate to the directory `Arcot-WebFort-5.4.1-Solaris/Misc`.

c. Uncompress the ODBC driver GZIP file, as follows:

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

d. Extract the resultant TAR file as follows:

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

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

   ii. Go to the `/opt` directory.

   ```
   prompt> cd /opt
   ```

   iii. Extract the content of the TAR file.

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

Requirements for Java-Dependant Components

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

1. JDK
2. Application Server

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

Chapter 4

Deploying WebFort on a Single System

This chapter guides you through installing and configuring WebFort for a single-system deployment.

The following steps provide a quick overview of the process:

- Execute the WebFort installer to add WebFort components to your file-system and configure them to access your SQL database. See **"Installing WebFort"** for install instructions.
- Execute the database scripts to create schema and database tables, see **"Running Database Scripts"**.
- Run the command line utility to configure Arcot's private OpenSSLCA, see **"Configuring OpenSSLCA"**.
- Deploy Administration Console in the application server, see **"Deploying Administration Console"**.
- Log in to Administration Console with the Master Administrator account to initialize WebFort and then create a Global Administrator. See **"Logging In to Administration Console"**.
- Deploy Sample Application for testing WebFort. It is also used as a code sample for integrating ArcotID authentication to your existing Web applications. See **"Deploying Sample Application"**.

The WebFort installer supports the following types of installation. You must use the *Complete* installation for single-system deployment.

1. **Complete** - Installs all WebFort components on a single system.
2. **Custom** - Installs the WebFort components that you select.

3. **Basic** - Installs only WebFort Server.

Important Notes Related to Installation

You must keep the following points in mind while installing WebFort on a single system:

- The *<install_location>* folder name must not contain any special characters (such as ~ ! @ # $ % ^ & * ( ) _ + = { } [ ] ’ ") and blank space.
- WebFort 5.4.1 does not support upgrade from a previous version (5.4 or earlier). Also, you can not install WebFort 5.4.1 over a previously installed version.
- Currently, you can not modify or repair WebFort components by using the installer. You *must* uninstall the component and then re-install it.
- Any time during installation, you can type `quit` and press **Enter** to exit the installation.

Installing WebFort

This section guides you through installing WebFort for a single-system deployment.

Before installing WebFort, ensure all the prerequisite software are installed and the database is set up, as described in the Chapter 3, "Preparing for Installation".

Perform the following steps to install WebFort and related components:

1. Log in to the Solaris OS.
2. Navigate to the folder where you untarred the installer.
3. Run the installer using the following command:

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

   The installer starts preparing for the installation.
4. If you are executing the installer with `root` login, then a warning message "You are installing as root" appears. To continue with the installation enter **Y** to continue or **N** to quit the installation. After specifying the required choice, press **Enter** to continue.

   The Welcome screen appears.
5. Press **Enter** to continue with the installation.

   The License Agreement for WebFort appears.
6. Press **Enter** until the license agreement is complete.

   At the end of the license agreement, the user is prompted for accepting the agreement.
7. Enter **Y** to accept the license agreement and continue with the installation.

   The Choose Installation Location screen appears.
8. Enter the absolute path of the folder, where the installation has to be performed. Else, press **Enter** to use the default path displayed.

   > **NOTE:** The installation folder name that you specify must not contain any spaces. This is because WebFort scripts and tools will not function as intended.
9. If the installation system has an already existing Arcot product, then the installer displays the following options:

a. 1 - Enter a new location.

b. 2 - Continue to install in the folder selected in **Step 8.**

c. 3 - Use the location at which the existing Arcot product is installed.

10. Select any of the preceding option and press **Enter** to continue with the installation.

    NOTE: If you have selected option 1 or 2, then a new folder `arcot` is created within the specified location.

    The Choose Install Type of Installation screen appears.

11. This screen displays the installation types provided by WebFort. Enter **1** to install all components of WebFort.

    The ODBC Home Configuration screen appears. This screen prompts the user for ODBC Driver path.

12. Enter the absolute path 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 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 the user for Oracle Client path.

13. Enter the path where the Oracle Client is available, and press **Enter** to continue.

    The installer checks for Oracle Client in the specified location. If multiple supported versions are found, then the installer displays all 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.

14. Enter the 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.

    If you are using JDK 1.5.x with Tomcat 5.5.x, then ensure the JAVA_HOME contains the java executable.

NOTE: This screen is displayed if the system does not have any Arcot product.

The Primary Database Access Configuration screen appears.

15. Perform the following steps on the Primary DSN screen:

    a. Enter the DSN name for the ODBC driver and press **Enter**. The recommended value to enter is `arcotdsn`.

       The installer checks for the availability of this DSN. If this DSN is already present, then it displays appropriate messages.

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

    c. Enter the other information as mentioned in the following table.

Table 4-1 Parameters for Oracle Database Access

Field	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. This name can be found in the `tnsnames.ora` file on the local system.
User Name	The User Name that WebFort uses to access the database. This name is specified by the database administrator. **NOTE:** The User Name for the Primary and Backup DSN should be different.
Password	The password that WebFort uses to access the database. This password is specified by the database administrator.
Service ID	The Oracle System Identifier that refers to the instance of the Oracle database running on the Oracle server.
Port No	The port at which the database server listens to the incoming requests.
Host Name	The host name of the computer where the Oracle server is available. **Syntax**: <Server Name> **Example**: demodatabase

Installer prompts for the database connectivity check using the database information provided.

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

The Backup Database Access Configuration screen appears.

16. Enter the information for backup DSN, if required. See sub-steps of **Step 15** for more information on the parameters.
17. Installer prompts to test the Backup DSN configuration. Enter **Y** to test, else **N** to continue.

    The WebFort Connectivity Screen appears.
18. Enter the Host Name and the Port number of WebFort Server. This information is used by Administration Console to authenticate administrators during logon.

    The Pre-Installation Summary screen appears. This screen lists the product name, installation folder, type of installation, components that are installed, and disk space information.
19. If you want to change any of the installation settings, then type **back** or press **Enter** to proceed with the installation.

    The Installation Complete screen appears at the end of successful installation.
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.

    NOTE: To view the complete history of all installation activity, refer to the log file `Arcot_WebFort_5.4.1_InstallLog.log at <install_location>/arcot/logs/.`

Post-Installation Tasks

The following post-installation tasks are discussed in this section:

1. Running Database Scripts
2. Testing the Installation
3. Configuring OpenSSLCA
4. Deploying Administration Console
5. Logging In to Administration Console
6. Creating a Domain Key
7. Creating a Global Administrator
8. Configuring TLS Communication (Optional)
9. Deploying Sample Application
10. Configuring Sample Application for WebFort Server
11. Using Sample Application

Running Database Scripts

WebFort ships with SQL scripts that create its schema and set initial configuration values in the Arcot database.

To configure the database used by WebFort:

1. Locate the folder with the scripts for your database. The default location is:

   `<install_location>/arcot/dbscripts/oracle`

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

   IMPORTANT: Before you run the scripts listed in this section, ensure that you are logged in as the same database user that you created in the "Configuring Database Server" section.

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

Testing 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 WebFort was installed correctly. Perform the following tasks to do so:

- Starting WebFort Server
- Stopping WebFort Server
- Verifying the Log Files

Starting WebFort Server

Perform the following steps to start WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following command:

   ```
   ./webfortserver start
   ```

After starting WebFort Server, you must check if it started successfully. To do so:

1. Navigate to the following directory:

   `<install_location>/arcot/logs/`

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

   ```
   Arcot WebFort Authentication Service READY
   ```

Stopping WebFort Server

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

Perform the following steps to stop WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following commands:

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

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

Verifying the Log Files

The log file that you need to verify if WebFort Server started correctly is:

- arcotwebfort.log

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

1. Navigate to the following location:

   <*install_location*>/arcot/logs/

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

   - STARTING Arcot WebFort 5.4.1_s
   - Arcot WebFort Authentication Service READY

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

Configuring OpenSSLCA

This section provides the steps to create new Issuer Root keypair and certificate. The Issuer certificate is used by Issuance to issue ArcotID certificates to users.

You can change the validity of CA before running the setup.sh script. By default the CA validity is configured to *365* days. Set the parameter days to the number of days required in the following line:

```
openssl req -config $CURDIR/ca.cnf -new -x509 -key
"$CURDIR/private/cakey.pem" -days 365 -out $CURDIR/cacert.pem
```

To generate the key pair:

1. Open a command prompt window on the computer where you are performing the installation.
2. Change to the following directory:

   <*install_location*>/arcot/sbin

3. Type . ./arctenv and press **Enter**.

4. Change to the following directory:

   `<install_location>/arcot/tools/opensslca`

5. Type `setup.sh` and press **Enter**.

6. Enter the responses to the queries as listed in the following table.

Table 4-2 Input Parameters for `setup.bat`

Parameters	Description
Country Name	Enter the name of your country. **Example**: US
State or Province Name	Enter the name of your state. **Example**: California
Locality Name	Enter the name of your city. **Example**: Sunnyvale
Organization Name	Enter the name of your organization. **Example**: SafeBank
Organizational Unit Name	It is recommended you leave this field blank as it is visible to end-users who will install the ArcotID Native client. You can optionally enter the name of the business unit that runs WebFort Server **Example**: IT Operations
Common Name	Enter the name of your organization. **Example**: SafeBank
Email Address	It is recommended you leave this field blank as it is visible to end-users who will install the ArcotID Native client. You can optionally enter email address of the support group in your organization. **Example**: support@safebank.com

7. Press **Enter** to continue.

   The CA key pair is generated with the inputs provided.

8. Close the command prompt window.

Deploying Administration Console

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

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

To deploy the Administration Console:

1. Deploy `arcotadmin.war` on the application server.

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

2. Change to the following directory:

   `<install_location>/arcot/sbin`

3. Type `. ./arctenv` and press **Enter**.

4. Start the application server.

Logging In to Administration Console

NOTE: You *must* start WebFort Server before logging in to Administration Console application.

When logging in to 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 Administration Console:

1. Open Administration Console in a Web browser window. The default URL for 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 Administration Console is deployed. For example, the default port for Tomcat is 8080.

2. Log in by using the default Master Administrator account credentials. The credentials are:

   - **User Name**: Master_Admin

- **Password**: master1234

3. Change the Master Administrator password after the first log in. Refer to the *Arcot WebFort 5.4.1 Administration Guide* for more information on changing the administrator password.

Creating a Domain Key

The main functionality of WebFort Server is to authenticate users. To authenticate to a domain, a user's ArcotID must be accredited to the domain. A *domain* is a group of servers to which users can authenticate. Each separate domain has one or more domain keys.

When an ArcotID is created, it is enabled for a set of domain keys. This allows the user to be authenticated by any WebFort Server that possesses a domain key from the set for the specific user. Therefore, WebFort should possess the corresponding Domain key in order to authenticate the users of that Domain.

To generate a Domain key:

1. Open Administration Console in a Web browser window.
2. Log in using Master Administrator credentials.
3. In the left pane, under **WebFort Configurations** click the **Generate Domain Key** link.

   The Arcot Domain Key creation form appears. See the following table for more information on the fields.

Table 4-3 Domain Key Creation Form fields

Form Fields	Description
Name	Enter the common name for the subject field of the domain key.
E-mail	You can enter email address of the support group in your organization. **Example**: support@safebank.com
Key Length	Select the length of the domain key. The Key can be 512, 1024 or 2048 bits in length.
Organization	Enter the name of your organization. **Example**: SafeBank
Organization Unit	You can enter the name of the business unit that runs WebFort Server **Example**: IT Operations

Table 4-3 Domain Key Creation Form fields

Form Fields	Description
State	Enter the name of your state.
Country	Enter the name of your country.
Validity End Date - [mm/dd/yyyy]	Specify the period for which the Domain Key is valid. Arcot recommends that Domain key be valid for at least for 5 years, this avoids frequent re-issue of ArcotIDs.
Password	Enter the password is used for secure storage of the domain key created. Provide a strong password to protect your domain key.
Confirm password	Re-enter the password to confirm it.

4. Fill the form and click the **Generate** button.

   On successful creation the "Domain-Key successfully generated" message appears.

5. Refresh WebFort Server after the Domain Key generation, so that it can authenticate ArcotID logins.

   Use the `aradmin` tool to refresh WebFort Server. Refer to the chapter *Tools for System Administrators* in *Arcot WebFort 5.4.1 Administration Guide* for more information on `aradmin` tool.

Creating a Global Administrator

Global administrators are responsible for configuring the system and performing the global settings, setting up the protocol, managing administrators and their credentials, and create next level of administrators.

> **NOTE:** Refer to *Arcot WebFort 5.4.1 Administration Guide* for more information on Global administrator privileges.

To create a GA account:

1. Open the Administration Console in a Web browser.

   The Arcot Administrator Login page appears.

2. Click the **Register Now** link and enroll a user.

3. Log in to Administration Console with Master administrator credentials.

4. In the left pane, under **Admin Configurations**, click the **Create Admin** link.

   The User Search page appears.

5. Enter the partial or complete information of the user (created in Step 2) who needs to be promoted to GA and click **Search**.

   A list of administrators matching the search criteria appears.

6. Click the **User Name** in the **Create Admin- Search Results** of the user you want to promote as administrator.

   The Create Admin page appears with the user name you have selected.

7. To specify the level of the administrator, select the policy to be associated.

   Select **Global Admin Policy**, from the **Policy** drop-down list to create a GA.

8. 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 Global Administrator.

9. The **Selected Groups** represents the groups that the newly created administrator will be managing. Select the group from the **Available Groups** and click the > button to add the group to the selected group.

10. Click the **Save** button, to create the GA.

    The "Admin Created Successfully" message appears.

Configuring TLS Communication (Optional)

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

- Between WebFort Server and Administration Console
- Between WebFort Server and Authentication SDK
- Between WebFort Server and Authentication Web Service

Between WebFort Server and Administration Console

To configure TLS-based communication between Administration Console and WebFort Server, you must configure WebFort Native protocol to TLS mode:

1. Open Administration Console in a Web browser.

2. Log in to Administration Console using a Global Administrator account. See "Creating a Global Administrator" for more information.
3. Under **WebFort Configurations** from the left-hand menu, select **Protocol Setup.**

   The WebFort Protocol Setup page appears.
4. Configure the WebFort Native protocol as follows:
   a. In the **Enable** column, ensure that the check box for the protocol to be enabled for TLS 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 SSL certificate chain for the server.

      NOTE: The certificates in the chain must start from Leaf certificate, Intermediate CA certificates, and then Root certificate.

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

      NOTE: The certificate chain and the private key, both *must* be in `.PEM` format and the private key uploaded must be not be password protected.
   d. Click **Save** to save the changes.
5. 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.
6. Restart WebFort Server, see "Stopping WebFort Server" and "Starting WebFort Server" for detailed steps.
7. Restart the application server.

Between WebFort Server and Authentication SDK

After setting up WebFort Server for TLS, you must setup a TLS communication between WebFort Server and Authentication Java SDK by configuring the `authenticator.properties` file at:

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

See **"authenticator.properties"** for more information on the configuration parameters.

Between WebFort Server and Authentication Web Service

After setting up WebFort Server for TLS, you must setup a TLS communication between WebFort Server and Authentication Web Services by configuring the `authenticator.properties` file at:

```
<ApplicationHome>/WEB-INF/classes/properties/authenticator.properties
```

Here, `ApplicationHome` represents the directory path where WebFort application WAR files are deployed.

See **"authenticator.properties"** for more information on the configuration parameters.

Restart the application server after you complete the configuration of the file.

Deploying Sample Application

> **NOTE:** If you are using *ArcotID Flash Client* for ArcotID operations mentioned in the following sections, then the Web Server must be enabled for HTTPS and Sample Application must be accessed over HTTPS.

Sample Application can be used for testing WebFort or as a code sample for integrating ArcotID authentication into existing web applications. Sample Application must be deployed in the same system where Authentication and Issuance SDK are Installed.

To deploy Sample Application:

1. Stop the application server.
2. Deploy the `webfort-5.4.1-sample-application.war` file from:

   `<install_location>/arcot/samples/java`
3. Navigate to **Settings** -> **Control Panel** -> **Administrative Tools** -> **Services.**
4. Locate and start the services of the application server.

NOTE: If you are using WebSphere, then you must restart the WebSphere server after you deploy the Sample Application WAR file.

Configuring Sample Application for WebFort Server

Configure the `authenticator.properties` file located at `<ApplicationHome>/WEB-INF/classes/properties/authenticator.properties` for Sample Application to communicate with WebFort Server. Here, `ApplicationHome` represents the directory path where WebFort application WAR files are deployed.

See "authenticator.properties" for more information on configuration parameters.

After configuring the `authenticator.properties` file, you must restart the application server to reflect the changes made.

Using Sample Application

This sub-section describes the ArcotID operations using Sample Application. If WebFort is installed successfully, then these operations must be executed without any error.

The following topics for Sample Application are covered in this section:

- Creating User and ArcotID
- Downloading ArcotID
- Authenticating using ArcotID

Creating User and ArcotID

To create a ArcotID:

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

   ```
   http://<host>:<port>/webfort-5.4.1-sample-application/index.jsp
   ```

   The WebFort 5.4.1 Sample Application page appears.

2. Click the **Create User/Create ArcotID** link

   The **Create User & ArcotID** page appears.

3. Enter the following information in this page:

   User Name: User name for the ArcotID.

   Password: Password for the ArcotID.

   Re-enter Password: Re-enter the same password for confirmation.

4. Click the **Create User** button to create the user.

Downloading ArcotID

To download the ArcotID:

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

   ```
   http://<host>:<port>/webfort-5.4.1-sample-application/index.jsp
   ```

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

   The Download ArcotID page appears.

2. Click the **Download ArcotID** link

   The **Download ArcotID** page appears.

3. Enter the user name of the ArcotID in the **Username** field.

4. Select the ArcotID Client type in the **Arcot Client Configuration** menu.

5. Choose the type of download for ArcotID in **Choose ArcotID download type** menu.

6. Click the **Download ArcotID** button to download the ArcotID.

Authenticating using ArcotID

To authenticate using the ArcotID:

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

   ```
   http://<host>:<port>/webfort-5.4.1-sample-application/index.jsp
   ```

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

   The Authenticate ArcotID page appears.

2. Click the **ArcotID Authentication** link

   The **ArcotID Authentication** page appears.

3. Select the ArcotID Client type in the **Arcot Client Configuration** menu.
4. Enter the user name for ArcotID in **Username** field.
5. Enter the password for ArcotID in **ArcotID Password** field.
6. Click **Authenticate** button to authenticate to WebFort.

Chapter 5

Deploying WebFort on Distributed Systems

This chapter guides you through installing and configuring WebFort for a distributed-system deployment or a high-availability deployment.

Following steps provide a quick overview of the process:

- Execute the WebFort 5.4.1 installer to add WebFort Server and Administration Console to your file system and configure them to access your SQL database. You can also choose to install the Web Services on the same system. See **"Installing on First System"** for install instructions.
- Execute the database scripts to create schema and database tables, see **"Running Database Scripts"**.
- Run the command line utility to configure Arcot's private OpenSSLCA, see **"Configuring OpenSSLCA"**.
- Deploy Administration Console in the application server, see **"Deploying Administration Console"**.
- Log in to Administration Console with the Master Administrator account to initialize WebFort and then create a Global Administrator. See **"Logging In to Administration Console"** for more information.
- Install the Java SDKs on one or more systems. See **"Installing on Second System"** for more information.
- Copy the configuration files from the system where WebFort Server is installed to the system where Java SDKs are installed. See **"Post-Installation Tasks for Second System"** for more information.
- Deploy Sample Application on a system where the Java SDKs are installed. See **"Deploying Sample Application"** for more information.

The WebFort installer supports the following types of installation. You must use the *Custom* installation type for distributed-system deployment.

1. **Complete** - Installs all WebFort components on a single system.
2. **Custom** - Installs the WebFort components that you select.
3. **Basic** - Installs only WebFort Server.

Important Notes Related to Installation

You must keep the following points in mind while installing WebFort in a distributed environment:

- The <*install_location*> folder name must not contain any special characters (such as ~ ! @ # $ % ^ & * ( ) _ + = { }[ ] ’ ") and blank space.
- WebFort 5.4.1 does not support upgrade from a previous version (5.4 or earlier). Also, you can not install WebFort 5.4.1 over a previously installed version.
- Currently, you can not modify or repair WebFort components by using the installer. You *must* uninstall the component and then re-install it.
- During Custom installation:
  - If you enter the number of main feature (`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.
- Any time during installation, you can type `quit` and press **Enter** to exit the installation.

Installing on First System

This section guides you through installing WebFort for a distributed-system deployment.

Before installing WebFort, ensure all the prerequisite software are installed and the database is set up, as described in the **Chapter 3, "Preparing for Installation"**.

Perform the following steps to install WebFort and related components:

1. Log in to the Solaris OS.
2. Navigate to the folder where you untarred the installer.
3. Run the installer using the following command:

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

   The installer starts preparing for the installation.
4. If you are executing the installer with `root` login, then a warning message "You are installing as root" appears. To continue with the installation enter **Y** to continue or **N** to quit the installation. After specifying the required choice, press **Enter** to continue.

   The Welcome screen appears.
5. Press **Enter** to continue with the installation.

   The License Agreement for WebFort appears.
6. Press **Enter** until the license agreement is complete.

   At the end of the license agreement, the user is prompted for accepting the agreement.
7. Enter **Y** to accept the license agreement and continue with the installation.

   The Choose Installation Location screen appears.
8. Enter the absolute path of the folder, where the installation has to be performed. Else, press **Enter** to use the default path displayed.

   > **NOTE:** The installation folder name that you specify must not contain any spaces. This is because WebFort scripts and tools will not function as intended.
9. If the installation system has an already existing Arcot product, then the installer displays the following options:

a. 1 - Enter a new location.

b. 2 - Continue to install in the folder selected in Step 8.

c. 3 - Use the location at which the existing Arcot product is installed.

10. Select any of the preceding option and press **Enter** to continue with the installation.

    NOTE: If you have selected option 1 or 2, then a new folder `arcot` is created within the specified location.

    The Choose Install Type of Installation screen appears.

11. This screen displays the installation types provided by WebFort. Enter **3** to install the selected components of WebFort.

    The Choose Product Features screen appears.

12. This screen displays all WebFort features. Enter the number corresponding to the feature that you wish to install.

    NOTE: Refer to "Important Notes Related to Installation" for more information on selecting the WebFort features for installation.

    Typically in the first system you install WebFort Server depending on how many systems you are distributing WebFort, Administration Console, and Authentication Web Service and Issuance Web Service. Press **Enter** to continue.

    The ODBC Home Configuration screen appears. This screen prompts the user for ODBC Driver path.

13. Enter the path 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 supported versions are found, then the installer displays all 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 the user for Oracle Client path.

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

    The installer checks for Oracle Client in the specified location. If multiple versions are found, then the installer displays all 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 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.

    If you are using JDK 1.5.x with Tomcat 5.5.x, then ensure the JAVA_HOME contains the java executable.

    NOTE: This screen is displayed if the system does not have any Arcot product.

    The Primary Database Access Configuration screen appears.

16. Perform the following steps on the Primary DSN screen:

    a. Enter the DSN name for the ODBC driver and press **Enter**. The recommended value to enter is `arcotdsn`.

       The installer checks for the availability of this DSN. If this DSN is already present, then it displays appropriate messages.

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

    c. Enter the other information as mentioned in the following table.

Table 5-1 Parameters for Oracle Database Access

Field	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. This name can be found in the `tnsnames.ora` file on the local system.
User Name	The User Name that WebFort uses to access the database. This name is specified by the database administrator. **NOTE:** The User Name for the Primary and Backup DSN should be different.
Password	The password that WebFort uses to access the database. This password is specified by the database administrator.
Service ID	The Oracle System Identifier that refers to the instance of the Oracle database running on the Oracle server.
Port No	The port at which the database server listens to the incoming requests.

Table 5-1 Parameters for Oracle Database Access

Field	Description
Host Name	The host name of the computer where the Oracle server is available. **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. Enter the information for backup DSN, if required. See sub-steps of **Step 16** for more information on the parameters.

18. Installer prompts to test the Backup DSN configuration. Enter **Y** to test, else **N** to continue.

    The WebFort Connectivity Screen appears.

19. Enter the Host Name and the Port number of WebFort Server. This information is used by Administration Console to authenticate administrators during logon.

    The Pre-Installation Summary screen appears. This screen lists the product name, installation folder, type of installation, components that are installed, and disk space information.

20. If you want to change any of the installation settings, then type **back** or press **Enter** to proceed with the installation.

    The Installation Complete screen appears at the end of successful installation.

21. 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.

> **NOTE:** To view the complete history of all installation activity, refer to the log file `Arcot_WebFort_5.4.1_InstallLog.log at <install_location>/arcot/logs/.`

Post-Installation Tasks for First System

The following post-installation tasks are discussed in this section:

1. Running Database Scripts
2. Testing the Installation
3. Configuring OpenSSLCA
4. Deploying Administration Console
5. Logging In to Administration Console
6. Creating a Domain Key
7. Creating a Global Administrator
8. Configuring TLS Communication (Optional)

Running Database Scripts

WebFort ships with SQL scripts that create its schema and set initial configuration values in the Arcot database.

To configure the database used by WebFort:

1. Locate the folder with the scripts for your database. The default location is:

   `<install_location>/arcot/dbscripts/oracle`

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

   IMPORTANT: Before you run the scripts listed in this section, ensure that you are logged in as the same database user that you created in the "Configuring Database Server" section.

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

Testing 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 WebFort was installed correctly. Perform the following tasks to do so:

- Starting WebFort Server
- Stopping WebFort Server
- Verifying the Log Files

Starting WebFort Server

Perform the following steps to start WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following command:

   ```
   ./webfortserver start
   ```

After starting WebFort Server, you must check if it started successfully. To do so:

1. Navigate to the following directory:

   `<install_location>/arcot/logs/`

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

   ```
   Arcot WebFort Authentication Service READY
   ```

Stopping WebFort Server

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

Perform the following steps to stop WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following commands:

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

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

Verifying the Log Files

The log file that you need to verify if WebFort Server started correctly is:

- arcotwebfort.log

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

1. Navigate to the following location:

   <*install_location*>/arcot/logs/

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

   - STARTING Arcot WebFort 5.4.1_s
   - Arcot WebFort Authentication Service READY

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

Configuring OpenSSLCA

This section provides the steps to create new Issuer Root keypair and certificate. The Issuer certificate is used by Issuance to issue ArcotID certificates to users.

You can change the validity of CA before running the setup.sh script. By default the CA validity is configured to *365* days. Set the parameter days to the number of days required in the following line:

```
openssl req -config $CURDIR/ca.cnf -new -x509 -key
"$CURDIR/private/cakey.pem" -days 365 -out $CURDIR/cacert.pem
```

To generate the key pair:

1. Open a command prompt window on the computer where you are performing the installation.
2. Change to the following directory:

   <*install_location*>/arcot/sbin

3. Type . ./arctenv and press **Enter**.

4. Change to the following directory:

   `<install_location>/arcot/tools/opensslca`

5. Type `setup.sh` and press **Enter**.

6. Enter the responses to the queries as listed in the following table.

Table 5-2 Input Parameters for `setup.bat`

Parameters	Description
Country Name	Enter the name of your country. **Example**: US
State or Province Name	Enter the name of your state. **Example**: California
Locality Name	Enter the name of your city. **Example**: Sunnyvale
Organization Name	Enter the name of your organization. **Example**: SafeBank
Organizational Unit Name	It is recommended you leave this field blank as it is visible to end-users who will install the ArcotID Native client. You can optionally enter the name of the business unit that runs WebFort Server **Example**: IT Operations
Common Name	Enter the name of your organization. **Example**: SafeBank
Email Address	It is recommended you leave this field blank as it is visible to end-users who will install the ArcotID Native client. You can optionally enter email address of the support group in your organization. **Example**: support@safebank.com

7. Press **Enter** to continue.

   The CA key pair is generated with the inputs provided.

8. Close the command prompt window.

Deploying Administration Console

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

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

To deploy the Administration Console:

1. Deploy `arcotadmin.war` on the application server.

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

2. Change to the following directory:

   `<install_location>/arcot/sbin`

3. Type `. ./arctenv` and press **Enter**.

4. Start the application server.

Logging In to Administration Console

NOTE: You *must* start WebFort Server before logging in to Administration Console application.

When logging in to 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 Administration Console:

1. Open Administration Console in a Web browser window. The default URL for 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 Administration Console is deployed. For example, the default port for Tomcat is 8080.

2. Log in by using the default Master Administrator account credentials. The credentials are:

   - **User Name**: Master_Admin

- **Password**: master1234

3. Change the Master Administrator password after the first log in. Refer to the *Arcot WebFort 5.4.1 Administration Guide* for more information on changing the administrator password.

Creating a Domain Key

The main functionality of WebFort Server is to authenticate users. To authenticate to a domain, a user's ArcotID must be accredited to the domain. A *domain* is a group of servers to which users can authenticate. Each separate domain has one or more domain keys.

When an ArcotID is created, it is enabled for a set of domain keys. This allows the user to be authenticated by any WebFort Server that possesses a domain key from the set for the specific user. Therefore, WebFort should possess the corresponding Domain key in order to authenticate the users of that Domain.

To generate a Domain key:

1. Open Administration Console in a Web browser window.
2. Log in using Master Administrator credentials.
3. In the left pane, under **WebFort Configurations** click the **Generate Domain Key** link.

   The Arcot Domain Key creation form appears. See the following table for more information on the fields.

Table 5-3 Domain Key Creation Form fields

Form Fields	Description
Name	Enter the common name for the subject field of the domain key.
E-mail	You can enter email address of the support group in your organization. **Example**: support@safebank.com
Key Length	Select the length of the domain key. The Key can be 512, 1024 or 2048 bits in length.
Organization	Enter the name of your organization. **Example**: SafeBank
Organization Unit	You can enter the name of the business unit that runs WebFort Server **Example**: IT Operations

Table 5-3 Domain Key Creation Form fields

Form Fields	Description
State	Enter the name of your state.
Country	Enter the name of your country.
Validity End Date - [mm/dd/yyyy]	Specify the period for which the Domain Key is valid. Arcot recommends that Domain key be valid for at least for 5 years, this avoids frequent re-issue of ArcotIDs.
Password	Enter the password is used for secure storage of the domain key created. Provide a strong password to protect your domain key.
Confirm password	Re-enter the password to confirm it.

4. Fill the form and click the **Generate** button.

   On successful creation the "Domain-Key successfully generated" message appears.

5. Refresh WebFort Server after the Domain Key generation, so that it can authenticate ArcotID logins.

   Use the `aradmin` tool to refresh WebFort Server. Refer to the chapter *Tools for System Administrators* in *Arcot WebFort 5.4.1 Administration Guide* for more information on `aradmin` tool.

Creating a Global Administrator

Global administrators are responsible for configuring the system and performing the global settings, setting up the protocol, managing administrators and their credentials, and create next level of administrators.

> **NOTE:** Refer to *Arcot WebFort 5.4.1 Administration Guide* for more information on Global administrator privileges.

To create a GA account:

1. Open the Administration Console in a Web browser.

   The Arcot Administrator Login page appears.

2. Click the **Register Now** link and enroll a user.

3. Log in to Administration Console with Master administrator credentials.

4. In the left pane, under **Admin Configurations**, click the **Create Admin** link.

   The User Search page appears.

5. Enter the partial or complete information of the user (created in **Step 2**) who needs to be promoted to GA and click **Search**.

   A list of administrators matching the search criteria appears.

6. Click the **User Name** in the **Create Admin- Search Results** of the user you want to promote as administrator.

   The Create Admin page appears with the user name you have selected.

7. To specify the level of the administrator, select the policy to be associated.

   Select **Global Admin Policy**, from the **Policy** drop-down list to create a GA.

8. 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 Global Administrator.

9. The **Selected Groups** represents the groups that the newly created administrator will be managing. Select the group from the **Available Groups** and click the > button to add the group to the selected group.

10. Click the **Save** button, to create the GA.

    The "Admin Created Successfully" message appears.

Configuring TLS Communication (Optional)

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

Between WebFort Server and Administration Console

To configure TLS-based communication between Administration Console and WebFort Server, you must configure WebFort Native protocol to TLS mode:

1. Open Administration Console in a Web browser.

2. Log in to Administration Console using a Global Administrator account. See **"Creating a Global Administrator"** for more information.

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

   The WebFort Protocol Setup page appears.

4. Configure the WebFort Native protocol as follows:

   a. In the **Enable** column, ensure that the check box for the protocol to be enabled for TLS 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 SSL certificate chain for the server.

      NOTE: The certificates in the chain must start from Leaf certificate, Intermediate CA certificates, and then Root certificate.

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

      NOTE: The certificate chain and the private key, both *must* be in `.PEM` format and the private key uploaded must be not be password protected.

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

5. 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.

6. Restart WebFort Server, see "Stopping WebFort Server" and "Starting WebFort Server" for detailed steps.

7. Restart the application server.

Installing on Second System

After installing WebFort Server and Administration Console, you must install the other components on the second system in this distributed-system deployment. 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 the prerequisite software components are installed on this system as described in **Chapter 3, "Preparing for Installation"**.

Perform the following steps to install WebFort components:

1. Navigate to the folder where you untarred the installer.
2. Run the installer using the following command:

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

   The installer starts preparing for the installation.
3. Follow the installer instructions from **Step 4** to **Step 11**.
4. In the Choose Product Features screen select the components you wish to install, typically you will be installing the Java SDKs or the Web Services for Authentication and Issuance.
5. After you have selected all the components, follow the steps from **Step 15** through **Step 21** to complete the installation.

Post-Installation Tasks for Second System

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

- Copying the Configuration Files
- Configuring TLS Communication (Optional)
- Working with Sample Application

Copying the Configuration Files

The following files must be copied from the system where Administration Console is installed to the system where Issuance SDK and Issuance Web Services are installed

NOTE: The folder path is same for the destination and source system.

a. `<install_location>/arcot/tools`

b. `<install_location>/arcot/certs`

Configuring TLS Communication (Optional)

Depending on whether you are using Java SDKs or Web Services refer to the following sections to configure SDKs for TLS transport mode:

- Between WebFort Server and Authentication SDK
- Between WebFort Server and Authentication Web Service

Between WebFort Server and Authentication SDK

To setup a TLS communication between WebFort Server and Authentication Java SDK, you must configure the `authenticator.properties` file at:

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

See "authenticator.properties" for more information on the configuration parameters.

Between WebFort Server and Authentication Web Service

To setup a TLS communication between WebFort Server and Authentication Web Services, you must configure the `authenticator.properties` file at:

`<ApplicationHome>/WEB-INF/classes/properties/authenticator.properties`

Here, `ApplicationHome` represents the directory path where WebFort application WAR files are deployed.

See "authenticator.properties" for more information on the configuration parameters.

Restart the application server after you complete the configuration of the file.

Working with Sample Application

Sample Application can be used for testing WebFort or as a code sample for integrating ArcotID authentication into existing web applications. The following topics for Sample Application are covered in this sub-section:

- Deploying Sample Application
- Configuring Sample Application for WebFort Server
- Using Sample Application

Deploying Sample Application

> **NOTE:** If you are using *ArcotID Flash Client* for ArcotID operations mentioned in the following sections, then the Web Server must be enabled for HTTPS and Sample Application must be accessed over HTTPS.

Sample Application can be used for testing WebFort or as a code sample for integrating ArcotID authentication into existing web applications. Sample Application must be deployed in the same system where Authentication and Issuance SDK are Installed.

To deploy Sample Application:

1. Stop the application server.
2. Deploy the `webfort-5.4.1-sample-application.war` file from

   `<install_location>/arcot/samples/java`
3. Navigate to **Settings** -> **Control Panel** -> **Administrative Tools** -> **Services.**
4. Locate and start the services of the application server.

   > **NOTE:** If you are using WebSphere, then you must restart the WebSphere server after you deploy the Sample Application WAR file.

Configuring Sample Application for WebFort Server

Configure the `authenticator.properties` file located at `<ApplicationHome>/WEB-INF/classes/properties/authenticator.properties` for Sample Application to communicate with WebFort Server.

Here, `ApplicationHome` represents the directory path where WebFort application WAR files are deployed.

See "authenticator.properties" for more information on configuration parameters.

After configuring the `authenticator.properties` file, you must restart the application server to reflect the changes made.

Using Sample Application

This sub-section describes the ArcotID operations using Sample Application. If WebFort is installed successfully, then these operations must be executed without any error.

The following topics for using Sample Application are covered in this section:

- Creating User and ArcotID
- Downloading ArcotID
- Authenticating using ArcotID

Creating User and ArcotID

To create a ArcotID:

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

   ```
   http://<host>:<port>/webfort-5.4.1-sample-application/index.jsp
   ```

   The WebFort 5.4.1 Sample Application page appears.

2. Click the **Create User/Create ArcotID** link

   The **Create User & ArcotID** page appears.

3. Enter the following information in this page:

   User Name: User name for the ArcotID.

   Password: Password for the ArcotID.

   Re-enter Password: Re-enter the same password for confirmation.

4. Click the **Create User** button to create the user.

Downloading ArcotID

To download the ArcotID:

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

   ```
   http://<host>:<port>/webfort-5.4.1-sample-application/index.jsp
   ```

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

   The Download ArcotID page appears.

2. Click the **Download ArcotID** link

   The **Download ArcotID** page appears.

3. Enter the user name of the ArcotID in the **Username** field.

4. Select the ArcotID Client type in the **Arcot Client Configuration** menu.

5. Choose the type of download for ArcotID in **Choose ArcotID download type** menu.

6. Click the **Download ArcotID** button to download the ArcotID.

Authenticating using ArcotID

To authenticate using the ArcotID:

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

   ```
   http://<host>:<port>/webfort-5.4.1-sample-application/index.jsp
   ```

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

   The Authenticate ArcotID page appears.

2. Click the **ArcotID Authentication** link

   The **ArcotID Authentication** page appears.

3. Select the ArcotID Client type in the **Arcot Client Configuration** menu.

4. Enter the user name for ArcotID in **Username** field.

5. Enter the password for ArcotID in **ArcotID Password** field.

6. Click the **Authenticate** button to authenticate to WebFort.

Chapter 6

Performing Basic Installation

This section will guide you through installing and configuring WebFort for Basic deployment. Following steps provide a quick overview of the process:

- Execute the WebFort 5.4.1 installer to add WebFort Server to your file system and configure them to access your SQL database. See **"Installing WebFort"** for install instructions.
- Perform the post-installation tasks, as describes in **"Post-Installation Tasks"** section.

The WebFort installer supports the following types of installation, you will be using the *Basic* installation type for this deployment.

1. Complete - Installs all WebFort Components on a single system
2. Custom - Installs the WebFort Components that you select
3. Basic - Installs only WebFort Server

Important Notes Related to Installation

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

- The `<install_location>` folder name must not contain any special characters (such as ~ ! @ # $ % ^ & * ( ) _ + = { } [ ] ' ") and blank space.
- WebFort 5.4.1 does not support upgrade from a previous version (5.4 or earlier). Also, you can not install WebFort 5.4.1 over a previously installed version.
- Currently, you can not modify or repair WebFort components by using the installer. You *must* uninstall the component and then re-install it.
- Any time during installation, you can type `quit` and press **Enter** to exit the installation.

Installing WebFort

WebFort Basic installation is required to support User name/password authentication to Administration Console.

This section guides you through the steps for installing WebFort on Solaris for your Basic deployment.

Before installing WebFort, ensure all the prerequisite software is installed and the database is set up, as described in the **Chapter 3, "Preparing for Installation"**.

Perform the following steps to install WebFort and related components:

1. Log in to the Solaris OS.
2. Navigate to the folder where you untarred the installer.
3. Run the installer using the following command:

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

   The installer starts preparing for the installation.
4. If you are executing the installer with `root` login, then a warning message "You are installing as root" appears. To continue with the installation enter **Y** to continue or **N** to quit the installation. After specifying the required choice, press **Enter** to continue.

   The Welcome screen appears.
5. Press **Enter** to continue with the installation.

   The License Agreement for WebFort appears.
6. Press **Enter** until the license agreement is complete.

   At the end of the license agreement, the user is prompted for accepting the agreement.
7. Enter **Y** to accept the license agreement and continue with the installation.

   The Choose Installation Location screen appears.
8. Enter the absolute path of the folder, where the installation has to be performed. Else, press **Enter** to use the default path displayed.

   > **NOTE:** The installation folder name that you specify must not contain any spaces. This is because WebFort scripts and tools will not function as intended.

9. If the installation system has an already existing Arcot product, then the installer displays the following options:

   a. 1 - Enter a new location.

   b. 2 - Continue to install in the folder selected in **Step 8.**

   c. 3 - Use the location at which the existing Arcot product is installed.

10. Select any of the preceding option and press **Enter** to continue with the installation.

    NOTE: If you have selected option 1 or 2, then a new folder `arcot` is created within the specified location.

    The Choose Install Type of Installation screen appears.

11. This screen displays the installation types provided by WebFort. Enter **2** to install WebFort Server.

    The Pre-Installation Summary screen appears. This screen lists the product name, installation folder, type of installation, components that are installed, and disk space information.

    NOTE: While performing WebFort Basic installation, if the corresponding DNS configuration has already been completed, then you will *not* be prompted for the DNS-related information (ODBC_HOME or JDBC_HOME). However, if the DNS has not already been configured, then you will need to specify this information in the additional screens that appear.

12. If you want to change any of the installation settings, then type **back** or press **Enter** to proceed with the installation.

    The Installation Complete screen appears at the end of successful installation.

13. 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.

    NOTE: To view the complete history of all installation activity, refer to the log file `Arcot_WebFort_5.4.1_InstallLog.log at <install_location>/arcot/logs/.`

Post-Installation Tasks

Perform the following post-installation tasks after installing WebFort:

- Testing the Installation
- Configuring TLS Communication (Optional)

Testing the Installation

After installation you must verify whether WebFort was installed correctly. Perform the following tasks to do so:

- Starting WebFort Server
- Stopping WebFort Server
- Verifying the Log Files

Starting WebFort Server

Perform the following steps to start WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following command:

   ```
   ./webfortserver start
   ```

After starting WebFort Server, you must check if it started successfully. To do so:

1. Navigate to the following directory:

   `<install_location>/arcot/logs/`

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

   ```
   Arcot WebFort Authentication Service READY
   ```

Stopping WebFort Server

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

Perform the following steps to stop WebFort Server:

1. Navigate to the following directory:

   `<install_location>/arcot/bin/`

2. Run the following commands:

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

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

Verifying the Log Files

The log file that you need to verify if WebFort Server started correctly is:

- `arcotwebfort.log`

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

1. Navigate to the following location:

   `<install_location>/arcot/logs/`

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

   - `STARTING Arcot WebFort 5.4.1_s`
   - Arcot WebFort Authentication Service READY

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

Configuring TLS Communication (Optional)

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

To configure TLS-based communication between Administration Console and WebFort Server, you must configure WebFort Native protocol to TLS mode:

1. Open Administration Console in a Web browser.

2. Log in to Administration Console using a Global Administrator account. See "Creating a Global Administrator" for more information.
3. Under **WebFort Configurations** from the left-hand menu, select **Protocol Setup.**

   The WebFort Protocol Setup page appears.
4. Configure the WebFort Native protocol as follows:
   a. In the **Enable** column, ensure that the check box for the protocol to be enabled for TLS 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 SSL certificate chain for the server.

      NOTE: The certificates in the chain must start from Leaf certificate, Intermediate CA certificates, and then Root certificate.

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

      NOTE: The certificate chain and the private key, both *must* be in `.PEM` format and private key uploaded must be not be password protected.
   d. Click **Save** to save the changes.
5. 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.
6. Restart WebFort Server as follows:
   a. Navigate to the following directory:

      `<install_location>/arcot/bin/`

b. Run the following commands:

```
./webfortserver stop
./webfortserver start
```

7. Restart the application server.

Chapter 7

Configuring APIs and Web Services

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

The chapter covers the following topics:

- Introduction to WebFort APIs
- Configuring Java APIs
- Configuring Web Services

Introduction to WebFort APIs

Authentication API

The Authentication API package provides the interface to integrate the two-factor authentication provided by WebFort with your application. The APIs also validates the supported user credentials.

The following are few of the operations that can be performed using authentication APIs:

- Verify the user credentials for supported authentication mechanisms, such as single step (User Name-Password, OTP) or multi step (ArcotID, QnA).
- Provide the Authentication Token after successful authentication.
- Verify the Authentication Tokens.

Issuance API

The Issuance API package takes care of the initial credential provisioning to the users. It also includes APIs for complete credential lifecycle management.

The following operations that can be performed by using Issuance APIs:

- Issuing the credentials to the users
- Performing the following credential lifecycle management operations:
    - Create
    - Revoke
    - Reissue
- Performing the user management
    - Create a user account
    - Update the user

Configuring Java APIs

This section provides the procedure to configure the Authentication and Issuance Java APIs so that they can be used with the your existing application.

- Configuring Authentication Java APIs
- Configuring Issuance Java APIs

Configuring Authentication Java APIs

Before proceeding with the configuration, ensure that the Authentication Java API package is selected and installed successfully during the WebFort installation.

> **NOTE:** The following instructions are based on 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.

To configure Authentication APIs for using in a J2EE Application:

1. Copy the following JAR files from `<install_location>/arcot` to `<ApplicationHome>/WEB-INF/lib` directory

   - `/sdk/java/lib/arcot/arcot_core.jar`
   - `/sdk/java/lib/arcot/arcot_wf_sdk.jar`
   - `/sdk/java/lib/external/commons-collections-3.1.jar`
   - `/sdk/java/lib/external/commons-lang-2.0.jar`
   - `/sdk/java/lib/external/commons-pool.jar`
   - `/sdk/java/lib/external/cryptix_old.jar`
   - `/sdk/java/lib/external/log4j-1.2.9.jar`

   In the target path, `ApplicationHome` represents the directory path where WebFort application WAR files are deployed.

2. If the application has an already configured `log4j` file, then merge it with the log configuration from

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

   Else rename `log4j.properties.wf_java_sdk` to `log4j.properties` and put it in `<ApplicationHome>/WEB-INF/classes/properties` directory.

3. Copy the configuration file `authenticator.properties` available at `<install_location>/arcot/sdk/java/properties` to `<ApplicationHome>/WEB-INF/classes/properties`.

   NOTE: To know more about APIs and their initialization, refer to the WebFort Javadocs at `<install_location>/arcot/docs/webfort/Arcot-WebFort-5.4.1-authentication-sdk-javadocs.zip`.

Configuring Issuance Java APIs

Before proceeding with the configuration, ensure the Issuance Java API package is selected and installed successfully during the WebFort installation.

NOTE: The following instructions are based on 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.

To configure Issuance APIs for using in a J2EE Application:

1. Copy the following JAR files from `<install_location>/arcot` to `<ApplicationHome>/WEB-INF/lib` directory

   - `/sdk/java/lib/arcot/arcot_cygnets.jar`
   - `/sdk/java/lib/arcot/arcot_core.jar`
   - `/sdk/java/lib/external/antlr-2.7.5.jar`
   - `/sdk/java/lib/external/asm.jar`
   - `/sdk/java/lib/external/bcprov-jdk14-131.jar`
   - `/sdk/java/lib/external/cglib-2.1.3.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/cryptix_old.jar
- /sdk/java/lib/external/dom4j-1.6.1.jar
- /sdk/java/lib/external/ehcache-1.1.jar
- /sdk/java/lib/external/hibernate3.jar
- /sdk/java/lib/external/jta.jar
- /sdk/java/lib/external/log4j-1.2.9.jar
- /sdk/java/lib/external/ojdbc14.jar
- /sdk/java/lib/external/sqljdbc.jar

In the target path, ApplicationHome represents the directory path where WebFort application WAR files are deployed.

2. If the application has an already configured log4j file, then merge it with the log configuration from <*install_location*>/arcot/sdk/java/properties/log4j.properties.issuance file.

   Else rename log4j.properties.issuance to log4j.properties and put it in <ApplicationHome>/WEB-INF/classes/properties directory.

   NOTE: To know more about APIs and their initialization, refer to the Issuance Javadocs at <*install_location*>/arcot/docs/webfort/Arcot-WebFort-5.4.1-issuance-sdk-javadocs.

Configuring Web Services

This section provides the procedure to configure the Authentication and Issuance Web services so that they can be used with the your existing application.

- Configuring Authentication Web Services
- Configuring Issuance Web Services

Configuring Authentication Web Services

Before proceeding with the configuration, ensure the Authentication Web services package is selected and installed successfully during the WebFort installation.

To configure the Authentication Web services:

1. Stop the application server.
2. Copy the `arcotwebfortws.war` file from `<install_location>/arcot/java/app/webfort` on application server.

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

3. Use the following WSDLs at the location `<install_location>/arcot/java/app/webfort` to generate the clients:
   - `AuthAccessorAPI.wsdl` (for SOAP 1.2)
   - `AuthAccessorAPISOAP11.wsdl` (for SOAP 1.1)
   - `AuthXActionAPI.wsdl` (for SOAP 1.2)
   - `AuthXActionAPISOAP11.wsdl` (for SOAP 1.1)
4. Configure the `authenticator.properties` file available at `<APP-SERVER-HOME>/webapps/arcotwebfortws/WEB-INF/classes/properties`. In this command, `APP-SERVER-HOME` represents the directory path where application server (for example, Apache Tomcat) is installed.

   See "authenticator.properties," for more information on the configuration parameters.

5. Start the application server.

Configuring Issuance Web Services

Before proceeding with the configuration, ensure the Issuance Web services package is selected and installed successfully during the WebFort installation.

To configure the Issuance Web services:

1. Stop the application server.
2. Deploy the `arcotregfortws.war` file from `<install_location>/arcot/java/app/webfort` on the application server.

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

3. Use the following WSDLs at the location `<install_location>/arcot/java/app/webfort` to generate the clients:
   - `AuthProvisionAPI.wsdl` (for SOAP 1.2)
   - `AuthProvisionAPISOAP11.wsdl` (for SOAP 1.1)
4. Start the application server.

Chapter 8

Uninstalling WebFort

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

The steps to uninstall WebFort on the Solaris platform are:

- Removing the Database
- Uninstalling WebFort
- Post-Uninstallation Steps

> **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 WebFort" to proceed with the uninstallation.

Perform the following tasks to uninstall the database:

1. Navigate to the following folder:

```
<install_location>/arcot/dbscripts/oracle/
```

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

   This deletes all the database tables.

Uninstalling WebFort

To uninstall WebFort, you need to remove the packages shipped with WebFort.

> **CAUTION:** Uninstallation of the packages, deletes the scripts required to uninstall the database. If you need to remove the WebFort Database, then refer to "Removing the Database" section before proceeding.

To uninstall WebFort Server on Solaris:

1. Log in to the Solaris OS.
2. Shut down the following components gracefully:
   - WebFort Server
   - Administration Console
   - Any application servers where other WebFort components are deployed
3. Ensure that all INI and other files related to WebFort are closed.
4. Navigate to the following directory:

   ```
   prompt> cd <install_directory>/arcot/"Uninstall_Arcot
   WebFort 5.4.1"
   ```

5. Run the uninstaller file using the following command:

   ```
   prompt> sh Uninstall_Arcot_WebFort_5.4.1
   ```

   The Uninstall Arcot WebFort 5.4.1 screen appears.
6. Press **Enter** to continue with the uninstallation.

   The Uninstallation Complete screen appears after uninstallation.

Post-Uninstallation Steps

The following are the post-uninstallation steps:

1. Delete the `<install_location>/arcot` folder.

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

2. Uninstall the following WAR files from `<APP-SERVER-HOME>/webapps`:

   - `arcotadmin.war` - Administration Console
   - `arcotwebfortws.war` - WebFort Server
   - `arcotregfortws.war` - Issuance
   - `webfort-5.4.1-sample-application.war` - Sample Application

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

   NOTE: If you have performed distributed-system deployment, then locate these WAR files on the system where you have deployed the particular component.

3. If Oracle Database was used for the database setup, then delete the file `tabspace_arrfreports.dat` from the system running the database.

Appendix A

WebFort File System Structure

This chapter provides the information about the location of all the files that are installed by the WebFort installer.

> **IMPORTANT:** In addition to the files and folders discussed in "WebFort File Structure", you will also see a blank file called **`arcotkey`** in the `arcot` folder. 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 folder 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.

WebFort File Structure

The following table lists the folder location for the commonly used files that are created by the installer.

Table A-1 Installation Directory Structure

Folder	File Description
<*install_location*>/arcot/bin	Contains the following executables: • aradmin • webfortserver • arversion • dbutil
<*install_location*>/arcot/dbscripts	Contains the SQL scripts to create the WebFort schema.
<*install_location*>/arcot/docs	Contains the Java and WSDL documents for Authentication and Issuance.
<*install_location*>/arcot/java/app	Contains the WAR and WSDL files required by WebFort, Issuance, and Administration Console.
<*install_location*>/arcot/lib	Contains WebFort Server binaries.
<*install_location*>/arcot/logs	Contains the installation and other log files.
<*install_location*>/arcot/plugins	Contains WebFort Server binaries.
<*install_location*>/arcot/sdk	Contains different SDKs supported by WebFort and dependant files.
<*install_location*>/arcot/certs	Contains all the server certificates.

Table A-1 Installation Directory Structure

Folder	File Description
<*install_location*>/arcot/conf	Contains the following configuration files: • arcotcommon.ini • webfortserver.ini • adminserver.ini • regfort.ini • jni.ini • securestore.enc
<*install_location*>/arcot/i18n	Contains the files required for internationalization of the product.
<*install_location*>/arcot/tools	Contains the opensslca tool.
<*install_location*>/arcot/samples	Contains the WAR file of WebFort Sample Application.
<*install_location*>/arcot/sbin	Contains the following files: • aradmin • arctenv • arversion • dbutil • util.wrapper • startupIssuanceServer.sh • watchdog • webfortserver.real
<*install_location*>/arcot/Uninstall_Arcot WebFort 5.4.1	Contains the executable that can be used to uninstall WebFort.

Appendix B

Configuration Files and Options

This appendix discusses the configuration files that WebFort uses and the parameters that you must configure in these files.

The following are the WebFort configuration files:

- **arcotcommon.ini**
- **webfortserver.ini**
- **adminserver.ini**
- **regfort.ini**
- **jni.ini**

The preceding files are installed to the following default location:

`<install_location>/arcot/conf`

- **authenticator.properties**
- **log4j.properties**

The preceding files are installed to the following default location:

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

INI Files

arcotcommon.ini

The `arcotcommon.ini` file contains parameters for the following configurations

- Database Settings
- LDAP Settings
- Instance Settings

Database Settings

The Database settings in the `INI` files allow you to identify the database to which the server is 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.

As with threads, configuring the maximum and minimum number of communication resources is a trade-off between maximizing server efficiency and maintaining system capacity. Specifically, each resource open on a server decreases the server's performance and there is a limit to the number of resources that can be open at a time before the system's performance falls below acceptable levels. At the same time, limiting the number of resources available limits the number of users that can be accessing the system at a time.

Maintaining unused communication resources between the server and the database is inefficient. At the same time, opening resources takes three times as many system resources compared to maintaining a previously opened resource. Therefore, opening and closing resources for each user is far less efficient than maintaining a pool of resources available at all times that can be shared by anyone accessing the system.

The trick is to maintain enough resources to handle average usage levels and allow enough resources to be opened to handle any peak load that the system might encounter.

Also, opening multiple resources at one time is more efficient than opening individual resources one at a time. Therefore, if demand occasionally spikes, it is more efficient to open multiple resources at one time than it is to open resources only as they are requested (in other words, multiple connections are opened simultaneously to handle the increased demand for resources).

> **NOTE:**
> Before you can specify the resources used by the server to communicate with the database, you must determine the estimated throughput for the system.

The following table lists the database setting parameters in the INI files and provides descriptions of each.

Table B-1 Database Setting Parameters in `arcotcommon.ini`

Parameter	Default	Description
`DbType`	oracle	The type of the database applicable to all database connections. The supported values are: • oracle • mssqlserver
`Driver`	No default	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` • SQLServer -> `com.microsoft.sqlserver.jdbc.SQLServerDriver`
`MaxConnections`	32	The maximum number of connections that are created between the server and the database. **Note**: There is a limit to how many connections a database server allows and this limit overrides the `MaxConnections` parameter. See your Oracle documentation for more information.
`MinConnections`	16	The minimum number of connections to initially create between the server and the database.
`IncConnections`	4	The number of connections that are created when a new connection is needed between the server and the database.

Table B-1 Database Setting Parameters in `arcotcommon.ini`

Parameter	Default	Description
`AutoRevert`	1	Specifies whether or not the system attempts 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 primary database after a failover occurs.
`MaxTries`	3	The number of times the server attempts 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 heartbeat checks on all the databases.
`Profiling`	0	Whether to log the database-related messages or not. Set to 1 if you want to enable logging of database-related messages.
`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 will be retried on the same database instance.
`TransactionRetrySleepTime`	10	The time difference between the transaction retries. This value is in millisecond.

Configuring Primary Database

The following table lists the parameters that define the configuration of the primary database.

Table B-2 Parameters for Primary Database Configuration

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 Name used by the server to access the database.

Configuring Secondary Database

A secondary database is mainly used during the failover. See the following table for more information on the parameters that define the configuration of the secondary database.

LDAP Settings

LDAP settings constitute information about the user directory and the attributes of the user stored in the directory. These settings are required by the Arcot authentication server to authenticate the user from these external user directories over the LDAP protocol.

The LDAP-related configurations are made in `[arcot/ldap]`. The following table describes the parameters used for this configuration.

Table B-3 LDAP Configuration Parameters

Parameter	Default	Description
`Timeout`	`30`	This configuration specifies maximum number of seconds to wait for search results. This parameter is in *seconds*.
`Host`	*`<LDAP server IP address>`*	The IP address of the LDAP server. This is a *mandatory* information.

Table B-3 LDAP Configuration Parameters

Parameter	Default	Description
`HostPort`	`389`	The port number of the LDAP sever.
`EnableLDAPAuth`	0	This configuration is to enable support for LDAP authentication for any group other than *Administrators*. Set this parameter to `1` to enable LDAP authentication or to `0` to disable.
`UserDN.<groupName>`	No default	This configuration specifies the user's DN in LDAP for a given group in Arcot DB. This parameter along with the user name will be used to bind the user. This is comma separated standard LDAP DN format. `$$UID$$` is used as the place holder where the user name is substituted to construct the complete DN for binding at run time. For example: `UserDN.GROUP2=cn=$$UID$$,cn=Manager,dc=arcotldap,dc=com`
`EnableLDAPQuery`	No default	This configuration is to enable support for LDAP query for ALL groups other than *Administrators*. Set this parameter to `1` to enable LDAP query or to `0` to disable.
`RootUser.<Group Name>`	No default	This is the complete DN for the user who has read access to the attributes of `UserDN.<Group Name>`. This information is required only if the LDAP query is enabled. Password for this user must be stored in `securestore.enc` file with the key `RootUser.<Group Name>`. Use `dbutil` tool for this operation.

Table B-3 LDAP Configuration Parameters

Parameter	Default	Description
`Attributes.<groupName>`	No default	This configuration specifies a set of attributes to be fetched from LDAP for the authenticated user and is required only if the LDAP query is enabled. The format for configuring the attributes for query, is a comma separated list of `<required attribute name>=<user attribute in LDAP>` For example: `Attributes.GROUP2=fname=cn,lname=sn,email=email` In the above example, `fname`, `lname`, and `email` are required attributes corresponding to the LDAP attributes `cn`, `sn`, and `email` respectively. **Note**: The `<Group Name>` is case-insensitive. But it must be same in all the entries.

Instance Settings

In a farm of servers it is recommended that every instance of the server has its own unique identification. Arcot supports a parameter to set and identify every instance of the servers, see the following table for parameter details.

Table B-4 Instance Settings in the INI File

Parameter	Default	Description
`InstanceId`	1	A 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.

webfortserver.ini

The `webfortserver.ini` file contains parameters for the following configurations

- Log File Settings
- Thread Settings

Log File Settings

WebFort records all system actions that have occurred in a file with a default name of `arcotwebfort.log`. 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 then records new actions in a new instance of `arcotwebfort.log`.

All the logging-related parameters are under the section `[arcot/webfort/logger]` in the `webfortserver.ini` file. The following table lists the log file setting parameters in the `webfortserver.ini` file and provides descriptions of each.

Table B-5 Log File Parameters in `webfortserver.ini`

Parameter	Default	Description
`Logfile`	`logs/arcotwebfort.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`.
`BackupLogFileDir`	`logs/backup` **Note:** This path is relative to `<install_location>/arcot/`	The location of the folder where backup log files are maintained after the current one exceeds `LogFileSize` bytes.

Table B-5 Log File Parameters in `webfortserver.ini`

Parameter	Default	Description
`LogLevel`	1	The default logging level for the server, unless an override is specified. The possible values are: • 0 FATAL • 1 WARNING • 2 INFO • 3 DETAIL
`LogTimeGMT`	0	The parameter that 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 are available for the system:

1. Each thread uses a specified 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 existing thread.
3. Based on the server's capacity, there is a maximum number of threads that can be created 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 might encounter while maintaining acceptable server performance.

The thread settings for WebFort can be found under the `[arcot/webfort/server]` section in the `webfortserver.ini` file. The following table lists the thread setting parameters in the `ini` files and provides descriptions of each.

Table B-6 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 contains parameters for the **Authentication Settings** configurations

Authentication Settings

Configure the location where WebFort Server is available, this configuration is done under the section `[arcot/admin/authconfig]`. The following table provides the configuration information.

Table B-7 Data Parameters for Authentication

Parameter	Default	Description
`remotehost.1`	<*Authentication server IP Address*>	IP address at which WebFort Server is available.
`remoteport.1`	<*PORT*>	Port at which WebFort Native protocol is listening.
`transport`	TCP	TCP is the default value for Administration Console to startup. Set this parameter to TLS if WebFort Native protocol is set to TLS mode. **NOTE:** If you change the transport mode to TLS, then you must restart WebFort Server.

Table B-7 Data Parameters for Authentication

Parameter	Default	Description
`server.CACert`	<server CA certificate (in PEM format) file path>	Provide the 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=<%SystemDrive%>/certs/webfort_ca.pem`

regfort.ini

The `regfort.ini` contains the parameter for configuring the JNI library path. You can configure under the section `[arcot/regfort/config]`. The following table describes all the parameters.

Table B-8 Parameters for JNI Configuration

Parameter	Default	Description
`JNI_LIBRARY_PATH`	No default	This parameter specifies the path in file system where the JNI libraries delivered with Arcot application is present. **NOTE:** This path should be different from the JNI library path for Administration Console.

jni.ini

The `jni.ini` file contains parameters for the following configuration:

- Log File Settings
- Configurations for OpenSSL CA
- Configuring Reusable Key Pair
- Configuration for Administration Console

Log File Settings

JNI records all system actions that have occurred in a file with a default name of `arcotjni.log`. 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 then records new actions in a new primary log file (new instance of `arcotjni.log`).

All logging-related parameters are under the section `[arcot/jni/logger]` 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 B-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`.
`BackupLogFileDir`	`logs/backup` **Note:** This path is relative to `<install_location>/arcot/`	The location of the folder 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

Table B-9 Log File Parameters in `jni.ini`

Parameter	Default	Description
`CreateLog`	1	The parameter that indicates whether the logging is enabled or not. The possible values are: • 0 OFF • 1 ON

Configurations for OpenSSL CA

All parameters required for the configuration of OpenSSL CA are under the section `[arcot/jni/opensslca]` in the `jni.ini` file. The following table lists the parameters for OpenSSL CA in the `jni.ini` file and provides descriptions of each.

Table B-10 Parameters for Openssl CA Configuration in `jni.ini`

Parameter	Default	Description
`ConfigFile`	`tools/openssl ca/ca.cnf` **Note:** This path is relative to `<install_location>/arcot/`	The file path to the default directory and the file name of the configuration file.
`PrivateKeyFile`	`tools/openssl ca/privatekey /cakey.pem` **Note:** This path is relative to `<install_location>/arcot/`	The file path to the default file that contains the Certificate Authority's private key.
`CACertFile`	`tools/openssl ca/cacert.pem` **Note:** This path is relative to `<install_location>/arcot/`	The location of the CA certificate file corresponding to the private key.

Table B-10 Parameters for Openssl CA Configuration in `jni.ini`

Parameter	Default	Description
`UseUTF8`	0	The parameter that indicates whether the data in the certificate should be in UTF-8 or ASCII format. The possible values are: • 0 OFF Text in ASCII format. • 1 ON Text in UTF-8 format.

Configuring Reusable Key Pair

The size of the key pair specified in this section is used to generate the ArcotID. This key pair is used every time the ArcotID is generated. See the following table for parameter details.

Table B-11 Parameters for Key Pair

Parameter	Default	Description
`PlainKeyBitSize`	1024	Size of the key pair used for ArcotID creation.

Configuration for Administration Console

The parameters required for 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 each.

Table B-12 Parameters for Administration Console Configuration

Parameter	Default	Description
`CertDirectory`	`certs/certificates` **Note:** This path is relative to `<install_location>/arcot/`	The default directory where the domain and Registration Authority (RA) certificates generated by the CA are stored.

Table B-12 Parameters for Administration Console Configuration

Parameter	Default	Description
RAStore	certs/p12stores/rastore.p12 **Note:** This path is relative to <install_location>/arcot/	When Administration Console requests RA store creation, the private key and certificate of RA are stored in this file. This is also used by Issuance to obtain the RA store location.
DomainStore	certs/p12stores/domainkeystore.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

authenticator.properties

The `authenticator.properties` file provides the parameters for Java SDKs and Web Services to read WebFort Server information. The following table lists the configuration parameters.

Table B-13 Parameters for `authenticator.properties` Configuration

Parameter	Default	Description
`remotehost.1`	`localhost`	IP address of system in which WebFort Server is installed.
`remoteport.1`	`9742`	Port number where the server is listening to.
`pool.maxactive`	`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.
`transport`	`TCP`	TCP is the default value for Administration Console to startup. To enable the TLS mode between WebFort Authentication SDK and WebFort Server set this parameter to `TLS`. **NOTE:** If you change the transport mode to TLS, then you must restart WebFort Server.
`server.CACert`	`<server CA certificate (in PEM format) file path>`	Provide the 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>/arcot/certs/webfort_ca.pem`

NOTE: The parameters in the file are separated by a semicolon.

log4j.properties

The `log4j.properties` file contains the log file information for Java applications. The following table provides information to configure `log4j.properties` file.

Table B-14 Parameters for `log4j.properties`

Parameter	Description
`log4j.appender.debuglog.File`	The name of the log file. Possible values for this parameter are: • `authsdk.log` -> for WebFort Java SDK • `arwebfortws.log` -> for WebFort Web Service • `arissuancews.log` -> for Issuance Web `Service` • `arcotissuance.log` -> for Issuance Java SDK
`log4j.appender.debuglog.MaxFileSize`	The file size of the log file. The default value is set to 10MB.
`log4j.appender.debuglog.MaxBackupIndex`	The index number to create the instance of the log file, if the log file is full.

Appendix C

Database Reference

WebFort Database contains a number of tables, some of which grow with increased usage of the product. This appendix describes the tables in WebFort 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 causes the tables to grow.

Because of restricted disk space, as a database administrator managing WebFort deployments, you might not want these tables to grow indefinitely. In this case, you can use the information in this appendix to truncate some tables to improve the database performance.

You must only truncate the tables that capture transaction details, such as audit log information. You *must not* truncate tables that capture user information, which is necessary for authentication.

> **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 adversely impacts performance during the delete process. Depending on the size of the rollback segments, this might 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 WebFort. This appendix also lists all tables used by WebFort and recommendations on truncating them. The following topics are covered in this appendix:

- **Database Sizing Calculations**
- **Database Tables and Truncating Recommendations**

Database Sizing Calculations

This section helps the database administrator to calculate the approximate size of the database that has to be set up for WebFort.

Denotations Used in Sample Calculations

The following denotations are used in the calculations:

- Number of users = *N*
- Average number of transactions per day = *T*
- Computation timeframe (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
- Computation timeframe (**D**) = 90 days

Sample Calculation 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 = `(21 * N)` KB
- Based on **daily activity**, the database size = `(T * D * 5)` KB

Database Tables and Truncating Recommendations

The following table lists all WebFort Database tables and their description.

Table C-1 WebFort Tables Information

Table Name	Description
ARSERVERS	This table contains the registration of Arcot product.
ARLOCALE	Contains the localization information.
ARCONFIG	Contains the global configurations.
ARCLIENTSSLROOTCAS	Contains path of the client Root CA certificate for two-way SSL.
ARPROTOCOLREGISTRY	Contains listener port information.
ARGROUP	Contains fixed configuration for a group.
ARSUBGROUP	Contains fixed configuration for a sub-group.
ARGROUPCONFIG	Contains configuration for a group.
ARSUBGROUPCONFIG	Contains configuration for a sub-group.
ARUSER	Maintains the user attribute information.
ARTXID	Maintains the cache of the unique Transaction ID per instance.
ARSERVERREGISTRY	Maintains the information about different instances of the components.
ARTRANSALGO	Contains pre-defined handlers for translating the credentials, for example, password, answers.
ARUSERPASSWORD	Contains user password credential.
AROTPTOKEN	Contains the one time token generated.
AROTP	Contains the user OTP credential.
ARARCOTWALLETS	Contains user ArcotID credential.
ARARCOTWALLETS_HISTORY	Contains user ArcotID credential for user's that have got ArcotID's reissued
ARQNATABLE	Contains the user QnA credential.
ARARCOTIDMGMTCONF	Contains ArcotID Issuance profiles.

Table C-1 WebFort Tables Information

Table Name	Description
ARQNAMGMTCONF	Contains QnA Issuance profiles.
ARPASSWORDMGMTCONF	Contains User Name -Password Issuance profiles.
AROTPMGMTCONF	Contains OTP Issuance profiles.
ARGROUPCREDENTIALS	Contains different Issuance profiles configured for a given group.
ARAUTHMECHANISMREGISTRY	Contains the list of different supported authentication mechanisms and corresponding handlers.
ARAUTHFWREGISTRY	Contains the handler for authentication framework.
ARCREDLOG	Contains audit information for the following Issuance activities: • Create • Reissue/reset • Delete
ARAUTHAUDITLOG	Contains audit information for each authentication activity.
ARVERIFIEDCHALLENGES	Contains information on the authentication challenges that are already verified.
ARRADIUSCONFIG	Contains information on RADIUS (NAS) clients configured for a VPN authentication.
ARRESOURCECATEGORY	Contains information about database resource types for all Arcot components.
ARACTIONCONSTANTS	Contains information about actions permitted on the DB resources.
ARPOLICIES	Contains information about the levels of administrators supported.
ARPRIVILEGE	Contains information about privileges for each level of administrator.
ARADMIN	Contains information about the existing administrators in the system.
ARADMINDOMAIN	Contains information about the GROUP(s) administered by an administrator.
ARADMINAUDITLOG	Contains activity logs for administrator actions.
ARCACHEREFRESH	Contains information needed to communicate cache refresh event across multiple Administration Console instances.

Tables That can be Truncated

The tables discussed in this section grow continuously with every transaction, but are not required for authentication. As a result, these can be truncated. These tables are:

> **NOTE:** Arcot highly recommends not to truncate the tables which are not mentioned in the list.

- **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.

- **ARAUTHAUDITLOG**

  This table contains the authentication information. By deleting entries from this table, the authentication history is reduced.

- **ARADMINAUDITLOG**

  This table contains the history of all the actions performed by administrators.

- **ARUSER**

It is highly recommended that you only truncate the tables that capture transaction details, such as audit log information. You *must not* truncate tables that capture the necessary user information.

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.

> **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 WebFort Issuance API.

Appendix D

Default Port Numbers and URLs

This appendix lists the default port numbers that WebFort uses. It contains the following sections:

- Default Port Numbers
- URLs for WebFort Components

Default Port Numbers

WebFort supports four protocols that are configured at different ports. Set each protocol to the port number as specified in Table D-1. You must specify the port number manually by using the WebFort Protocol Setup screen in WebFort Administration Console.

The following table lists the default port numbers used by WebFort.

Table D-1 Default Port Numbers

Protocol Module	Default Port Number	Description
WebFort Native	9742	This protocol is a proprietary binary protocol supported by WebFort. Applications integrating with WebFort can use this protocol to communicate with WebFort Server.
WebFort ASSP	9741	This protocol is used with Adobe® Reader and Adobe® Acrobat® to digitally sign the PDF documents on the server.
WebFort RADIUS	1812	This protocol supports the standard RADIUS protocol. It is used to support the RADIUS protocol. Applications integrating with WebFort communicates with the server using RADIUS.
Server Management	9743	This protocol is used for the management of WebFort Server. Currently, the protocol supports server cache refresh and shut-down requests.

URLs for WebFort Components

Use the URLs listed in the following table to access WebFort components after installation. The URLs in the table use the default ports.

Table D-2 Default Port Numbers

Component or Service	URL
Administration Console	`http://<AppHost>:<port>/arcotadmin/adminlogin.htm`
Issuance Web service	`http://<AppHost>:<port>/arcotregfortws/services/AuthProvisionAPIService`
Sample Application	`http://<AppHost>:<port>/webfort-5.4.1-sample-application/index.jsp`
Authentication Web service	`http://<AppHost>:<port>/arcotwebfortws/services/AuthXActionService`
Web service for ArcotID download	`http://<AppHost>:<port>/arcotwebfortws/services/AuthAccessorService`
Issuance WSDL file	`http://<AppHost>:<port>/arcotregfortws/services/AuthProvisionAPIService?wsdl`
Authentication WSDL file	`http://<AppHost>:<port>/arcotwebfortws/services/AuthXActionService?wsdl`
WSDL file for ArcotID download	`http://<AppHost>:<port>/arcotwebfortws/services/AuthAccessorService?wsdl`

Appendix E

Third-Party Software Licenses

This appendix lists the third-party software packages that are used by WebFort. These include:

OpenSSL

Oracle Database 10*g* JDBC Driver

Hibernate Core 3.1

Cryptix

dom4j

Apache

- `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)

Spring Framework

Copyright © 2006-2008, SpringSource, All Rights Reserved. The Spring Framework is licensed under the terms of the Apache License, Version 2.0.

Bouncy Castle

Copyright © 2000 - 2006 The Legion Of The Bouncy Castle.

Sun Microsystems

Copyright © 1994-2007 Sun Microsystems, Inc. All Rights Reserved.

- Java Mail (Copyright © 1994-2008 Sun Microsystems, Inc.)
- JSTL (Copyright © 1994-2008 Sun Microsystems, Inc.)

ANTLR 2

Copyright © 2003-2006, Terence Parr. Public-domain software.

Appendix F

Glossary

3DES	3DES is a block cipher formed from the Data Encryption Standard (DES) by using it three times. There are variations of 3DES which use two different keys and three different keys (3DES)
ArcotID Domain	A domain is a group of servers to which users might authenticate using the ArcotID.
ArcotID Domain Key	The domain key is a key issued to a Domain. When an ArcotID is created, it is enabled for a set of domain keys. The domain key is used during authentication to encrypt/decrypt the public key stored in the certificate.
ArcotID	Is a secure software credential that allows hardware level authentication in software form.
Authentication	Is 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.
Credential	A proof of user identity. Digital credentials might be stored on hardware such as smart cards or USB tokens or on the server. They are verified during authentication.
Cryptographic device	Hardware device used to store the user sensitive keys.
cryptographic hash function	A cryptographic hash function is a hash function with additional security properties, used in security-related applications such as authentication.
Customer Support Representatives (CSR)	CSRs are the administrators responsible for the day-to-day operations related to users of the security system. For example, Administrators can assist users with enrollment, reset users passwords, and view a variety of enrollment reports.
Digest-MD5	Is a widely used cryptographic hash function with a 128-bit hash value.

digital certificates	A certificate is 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 PKI cryptography method.
encryption	The process of scrambling information in a way that disguises its meaning.
Error Message	Message returned by application to report to the user agent regarding any erroneous situations.
Forgot Your Password (FYP)	If the user forgets his ArcotID password, then a QnA session is carried out between the User and WebFort. On answering a minimal set of questions, the user is asked for a new ArcotID password and a new ArcotID is issued.
Global Administrator	An administrator responsible for setting up CSR Administrator accounts and configuring the system.
N-Strikes	The maximum number of failed authentication attempts that can be made by the user before locking out.
PKCS	PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA. See "**public-key cryptography,**" for more details.
PKCS#12	Defines a file format commonly used to store private keys with accompanying Public key certificates protected with a password-based symmetric key.
PKCS#15	Defines a standard allowing users of cryptographic token to identify themselves to applications, independent of the application's cryptoki implementation or other API.
private key	One of a pair of keys used in public-key cryptography. The private key is kept secret and can be used to decrypt/encrypt data.
public key	One of a pair of keys used in public-key cryptography. The public key is distributed freely and 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.
public-key cryptography	Public-key cryptography is a form of modern cryptography which allows users to communicate securely without previously agreeing on a shared secret. Unlike symmetric cryptography, it uses two keys -- a public key known to everyone and a private or secret key known only to the owner of the public and private key pair. Public key cryptography is also called asymmetric cryptography.

QnA	An authentication mechanism, QnA allows for a back and forth dialog between the user agent and server, where the server asks arbitrary number of questions, and the user supplies correct answers.
Secure Hash Algorithm (SHA)	Secure Hash Algorithm (SHA) family is a set of cryptographic hash functions.
Single Sign-On (SSO)	SSO refers to a single identity that is shared across multiple systems. SSO lets a user logon once to a computer or network and access multiple applications and systems using a single credential.
Transport Layer Security (TLS)	TLS is a protocol intended to secure and authenticate communications across public networks by using data encryption.
User Name-Password	One of the credential issued to the user during enrollment.
WebFort	WebFort Server authenticates the end users with the help of user credentials which are issued by Issuance.
Web Services Definition Language (WSDL)	A standard XML format prescribed by W3C to describe network services as collections of communication end points capable of exchanging messages. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. A WSDL document describes a Web Service and specifies the location and the methods that the service exposes.
Web Services Security (WS-Security)	This is a communication protocol providing a means for applying security to Web services.

Index

A

about this guide 5
Administration Console
    bootstrapping 45, 65
    configuration 45, 65, 108
    getting started 45, 65
    log file 45, 65
adminserver.ini 108
arcotcommon.ini 100
Authentication
    API 84
        configuring 85
    Web services
        configuring 88
Authenticator.properties 114

C

complete install 37, 57
configuration
    Administration Console 108
configuration files 99
Configuring Administration Console 45, 65

D

database setup 31
    Oracle 31
deployment models 16
    basic 23
    distributed system 19
    high availability 22
    single system 16
domain 46, 66
Domain key 46, 66

H

hardware requirements 26

I

INI files 99
    adminserver.ini 108
    arcotcommon 100
    database settings 100
    jni.ini 109
    regfort.ini 109
    webfortserver.ini 105
installation directory 96
installing
    complete 37, 57
    distributed-system
        second system 70
intended audience 5
Issuance
    API 84
        configuring 86
    Web services
        configuring 89

J

jni.ini 109

L

log file 106, 110
log4j.properties 115

P

Patents ii
Post installation tasks

Configuring Administration Console 45, 65
prerequisite software 26
properties files 114, 115

R

regfort.ini 109

T

Third party software ii
thread settings 107
Trademarks ii

U

URLs 125

W

WebFort
configuration
instance setting 105
thread settings 107
webfortserver.ini 105