Arcot WebFort® Installation and Deployment Guide (for Windows)

Version 6.0

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot WebFort Installation and Deployment Guide
Version 6.0
August 2009
Part Number: AWF01-002DC-06000

Trademarks

Patents

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

The Arcot WebFort 6.0 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 administrators, database administrators, system integrators, Web developers, and others who are responsible for the installation, deployment, and maintenance of Arcot WebFort.

Information Included in this Guide

This guide is organized as follows:

- **Chapter 1, "Understanding WebFort VAS® Basics",** provides an overview of WebFort, key concepts, and the new features in the current version.
- **Chapter 2, "Planning the Deployment",** describes 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, "Configuring Java SDKs and Web Services",** describes the steps to configure the APIs and Web services provided by WebFort.
- **Chapter 7, "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 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, "Configuring Application Server",** describes the application server configuration that must be made for connection pooling.
- **Appendix F, "Configuring for SSL",** describes how to set up SSL communication between WebFort Server and the clients.
- **Appendix G, "Third-Party Software Licenses",** lists the license text of third-party software packages that are used by WebFort.
- **Appendix H, "Glossary",** lists the key terms related to WebFort.

Related Publications

Other related publications are as follows:

Arcot WebFort 6.0 Administration Guide	This guide includes the information to administer and configure WebFort.
Arcot WebFort 6.0 Java Developer's Guide	This guide describes the Java APIs provided by WebFort and also explains how to use them.

Arcot WebFort 6.0 Business Logic Extension Guide	This guide provides information about how to write a plug-in or callout to extend the existing authentication and issuance processes.
ArcotID Client 6.0 Reference Guide	This guide describes ArcotID Client types and the APIs provided by the client.
ArcotID Flash Client 6.0 API Guide	This guide explains the ArcotID Flash client APIs provided by the client.

Conventions Used in This Book

The following typographical conventions are used in this guide.

Type	Usage	Example
Bold	Screen Items	Click the **Install** button to install the product.
Italic	Key Words	First time log in to the *Administration Console* must be done using Master Admin credentials.
	Names of Publications	For more information, see the *Arcot WebFort 6.0 Administration Guide*.
	Emphasis	*Never* give anyone your password.
Cross reference	Links in the guide	Refer to the section Deployment Overview 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`

Contacting Support

If you need help, contact Arcot Support as follows:

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

Chapter 1

Understanding WebFort VAS® Basics

With the exponential increase in cases of Internet-based fraud over the last few years, relying just on user name-password for authentication is no longer sufficient. The need for stronger authentication can either be to protect end users or to comply with government-mandated security requirements, internal policies, or best practices. However, adding stronger authentication often creates conflict between compliance requirements and user convenience. In other words, organizations must increase the security of their authentication processes by reducing the complexity, and reduce the risk of financial losses or brand damage by increasing the customer and partner access to applications and data.

Arcot WebFort Versatile Authentication System® (VAS) is a trusted strong authentication service that enables your application to verify and protect the identity of your end users:

- By not transmitting passwords (either in clear or encrypted) over the network.
- By enabling you to choose the authentication method that best suits the security and convenience needs of different types of users.
- By using ArcotID®, which is based on patented **Cryptographic Camouflage** technique to protect private keys.

  In *Cryptographic Camouflage*, the private keys are not encrypted with a password that is too long for exhaustive attacks. Instead, private keys are encrypted such that only one password will decrypt it correctly, but many passwords will decrypt it to produce a key that looks valid enough to fool an attacker. As a result, this method protects a user's private key against dictionary attacks and the Man-in-the-Middle (MITM) attacks, as a smart card does, but entirely in software.

The biggest advantage of WebFort is that it enables you to upgrade security from simple user name-password authentication without changing the user login experience or critical business processes by using an ArcotID for authentication.

This chapter introduces you to **WebFort as a Versatile Authentication Server**, its component architecture (**WebFort Architecture**), and lists the new features and enhancements introduced this release (**What's New in this Release**).

WebFort as a Versatile Authentication Server

WebFort is a *Versatile Authentication Server* (*VAS*) because it supports the implementation of a wide range of proprietary and open authentication mechanisms. It not only supports authentication by using public-key credentials (PKCS) and one-time password (OTP), but it is also designed to plug in any existing authentication methods, if required, thereby enabling your organization to handle changes to critical systems and partner applications seamlessly.

As a result, the VAS functionality of WebFort provides your organization the complete flexibility to choose the authentication method that best suits the needs of your end users. You can choose to:

- Integrate with a variety of standard authentication interfaces.
- Implement standards-based hardware or software authentication methods.
- Add new authentication methods, such as the ArcotID, while continuing to support legacy technology, such as one-time password (OTP) tokens.
- Extend WebFort VAS through Plug-in or Callouts to do proprietary authentication.

Plugging Into WebFort

WebFort provides the following authentication methods out of the box:

- ArcotID
- User Name-Password
- One-Time Password
- Question and Answer (QnA)
- LDAP User Name-Password

If you want to implement any mechanisms other than these, then WebFort provides you the flexibility to do so either by writing **Callouts**, **Plug-Ins,** or by using **Custom APIs**.

Callouts

A Callout is a custom component (which can be written in a programming language of your choice) to modify or augment the standard functionality of WebFort. A *Callout* is an external process. As a result, it resides outside of the WebFort Server context and is hosted on a separate HTTPS-based server.

Because a Callout is an external process, you need not register it. However, you must configure it (by using the Administration Console) for a published set of events, so that it is invoked when the specified event occurs.

> **NOTE:** See the *Arcot WebFort 6.0 Business Logic Extension Guide* for details on how to write a Callout. Also, see the *Arcot WebFort 6.0 Administration Guide* for detailed steps on configuring the Callout.

You can configure multiple Callouts for one organization, and you can also configure the same plug-ins for multiple organizations.

Plug-Ins

Like a Callout, a *Plug-in* is also a custom server-side component, written in C or C++, that enables you to extend the functionality of WebFort VAS. However unlike a Callout that is an external process, a plug-in is a server-side process and is implemented as a custom event handler library within the context of the WebFort Server.

Unlike a Callout, you must register your plug-in (by using the Administration Console) to a published set of events, so that the plug-in is invoked when the specified event occurs.

NOTE: See the *Arcot WebFort 6.0 Business Logic Extension Guide* for details on how to write a plug-in. Also, see the *Arcot WebFort 6.0 Administration Guide* for detailed steps on registering and configuring the plug-in.

You can configure multiple plug-ins for one organization, and you can also configure the same plug-in for multiple organizations.

Custom APIs

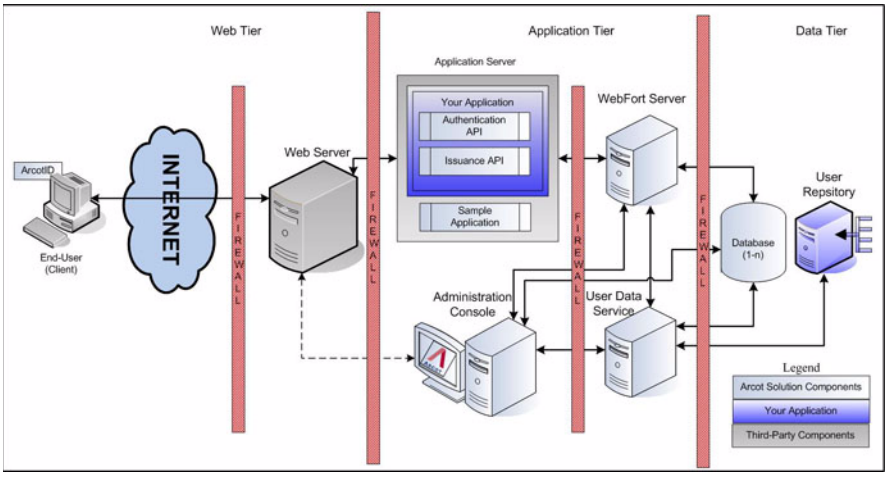
WebFort enables you to implement authentication methods other than the default supported methods. For example, hardware-based authentication using tokens, or certificate-based authentication. To handle such credentials, WebFort provides APIs (`CustomIssuance` and `CustomAuth`) to create and mange these credential, and authenticate them.

WebFort Architecture

You can install WebFort on a single system or you can distribute its components across multiple systems. However, to ensure maximum security of transactions, Arcot recommends the architecture shown in Figure 1-1 with the following three layers:

- Web Tier
- Application Tier
- Data Tier

Figure 1-1 WebFort Architecture Diagram



The following subsections discuss the WebFort components in each of these layers.

Web Tier

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

This layer serves the ArcotID Client (Java, Flash, or Native) to the end user's browser. ArcotID Client interacts with the WebFort Server for user authentication. It collects the ArcotID password, signs the challenge, and then sends the signed challenge to the WebFort Server for verification.

> **NOTE:** See the *ArcotID Client 6.0 Reference Guide* for details on ArcotID Client.

Application Tier

This layer constitutes WebFort Server, your application that uses WebFort SDKs, and the application servers where the Administration Console and the User Data Service (UDS) reside.

> **NOTE:** All components in this layer can be installed on one system or can be distributed across multiple systems.

- **WebFort Server**

  Server component that processes issuance and authentication requests from your application through WebFort SDKs.

- **Administration Console**

  Web-based console for configuring server instances, communication mode between WebFort components, authentication policies, managing credentials, and for managing organizations, administrators, and users.

- **User Data Service**

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

- **Authentication SDK**

  APIs that can be invoked by your application to forward authentication requests to WebFort Server.

- **Issuance SDK**

  APIs that can be invoked by your application to forward issuance requests to WebFort Server for enrolling users and for creating and managing their credentials in WebFort.

- **Sample Application**

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

Data Tier

This tier comprises the Relational DataBase Management Systems (RDBMSs) that WebFort uses to store the configuration, and credential, and user data if other user repositories are not configured.

What's New in this Release

The key features and enhancements in the WebFort 6.0 release include:

- **Support for Multiple Organizations**

  This release provides enterprises the ability to map their existing organization structure in WebFort, and to define the authentication and issuance policies either for each organization individually, or globally for all organizations.

  WebFort also offers the capability to allow user membership in different organizations and supports various configurations for these organizations.

- **Support for Versatile Authentication**

  The WebFort architecture is extensible to support a wide range of authentication mechanisms, ranging from simple username-password authentication to complex multifactor authentication. In addition to using the out-of-box strong-authentication capability, this release also enables you to extend the WebFort authentication and issuance functionality by using any of the following methods:

  - **By Adding Callouts**

    To add the Callouts, you can write you custom authentication logic in *any* programming language of your choice and host it on a separate HTTPS-based server.

  - **By Adding Plug-Ins**

    To add plug-ins, you must write your custom authentication logic in C or C++ and integrate your code with the SDKs provided by WebFort.

  - **By Adding New (or Custom) SDKs**

    Instead of just modifying the existing SDKs shipped with WebFort, this release also provides the flexibility to write completely new authentication and issuance functionality.

- **Integration with LDAP Directory Servers**

  With this release, WebFort can also connect to the LDAP directory servers (in addition to the supported SQL databases) for fetching user information. As a result, this integration ensures a single source for all the user-specific data. The process of integrating WebFort to the existing LDAP directory is easy and seamless and is done by using the Administration Console.

  NOTE: To support this feature, the user search feature is enhanced and also new screens are added to map the Arcot and LDAP attributes.

- **Enhancements in Administration Console**

  In this release, the Administration Console Graphical User Interface (GUI) has been improved to a tabbed interface, which makes the navigation through the console easy. The Administration Console now also supports:

  - Organization-related configurations, which includes:
    - ArcotID Profile Configuration
    - QnA Profile Configuration
    - Username-Password Profile Configuration
    - OTP Profile Configuration
    - ArcotID Authentication Policy Configuration
    - QnA Authentication Policy Configuration
    - Username-Password Authentication Policy Configuration
    - OTP Authentication Policy Configuration
    - SAML Token Configuration
    - ASSP Configuration
  - Common configurations, which includes:
    - Protocol Configuration
    - Instance Configuration
    - Server Connectivity Configuration

- **Maintenance of Configuration Versions**

  Starting with this release, all configuration versions are maintained. This enables you to track all the configuration changes that are done by using Administration Console.

- **Support for Instance Management**

  WebFort now provides a comprehensive screen as well as the **`arwfclient`** tool that you can use to manage the WebFort Server instances that you have deployed. Using this screen, you can perform the following instance management operations:

  - Configure Instance-level configuration parameters, such as log file, log level, different trace, and database connection pool configuration.

- Refresh the server cache.
- Gracefully shut down the server.
- Configure the server port (only through the Administration Console.)
- Fetch detailed statistical information of the server.

- **Support for Two-Way SSL Communication**

  Starting with this release, WebFort supports two-way SSL communication between all its components. This is an optional configuration, and is supported between:

  - Authentication Java SDK to Server
  - Issuance Java SDK to Server
  - Administration Console to Server
  - Server to UDS (that handles user repositories, such as LDAP and database)

- **Simplified Installation and Deployment**

  A number of manual installation and configuration steps have been automated in this release. As a result, there are fewer installation screens now.

- **ArcotID Enhancements**

  - **Support for ArcotID Renewal**

    You can now configure a warning period (by using the Administration Console) before an ArcotID is about to expire. When the ArcotID life span reaches this warning period, WebFort alerts your application about the ArcotID expiry. Your application can then prompt the user for new password and renew the ArcotID with this password.

  - **Support for ArcotID Grace Period**

    You can now configure a grace period for ArcotID, which implies that users can continue to authenticate with an expired ArcotID till this grace period is completed. However, this feature must be used judiciously.

  - **Enabling ArcotID Auto-Update**

    In case a user is authenticating by using an older version of the ArcotID, WebFort now fails the authentication and returns a specific code to the application, so that the application can handle it and update the ArcotID on the user's system.

This feature is also useful for the users who use ArcotID on more than one system. In this case if they change the ArcotID password on one system, then the password for the ArcotID on the other systems is automatically updated.

- **Support for ArcotID Attributes**

  WebFort now allows you to set ArcotID attributes, outside the certificate. You can configure these attributes either while creating the ArcotID or later by using the relevant API.

- **ArcotID Configurations to be Stored in the Database**

  Starting with this release, all ArcotID-related configurations except the database-related configurations will be stored in the WebFort database. This makes the management of these configurations in multiple-system deployment relatively easier.

- **Issuance Enhancements**

  - **Issuance Functionality Moved to Server**

    The Issuance function has been moved to the WebFort Server. This change makes the Issuance Java SDK very "thin" and also enables you to easily upgrade or migrate your application to the newer versions of WebFort SDK with less impact.

    NOTE: If you are using the Issuance Java SDK provided with previous releases, then you *must* use the new JAR file(s). Refer to **Chapter 6, "Configuring Java SDKs and Web Services"** for specific details on which new files to use and the corresponding configuration changes to make.

  - **Support for User Checks During Issuance**

    WebFort now verifies the user status (users in ACTIVE state only) and attributes as a pre-condition for creating credentials for users. Any of the mapped attributes can be used for enforcing the check.

    This feature is useful while migrating users from an existing authentication mechanism to WebFort strong authentication.

- **Credential Enhancements**

  - **Support for User and Credential Management**

    By using the WebFort Administration Console, you can not only view the user details, but also their credential details by using the User Search functionality. You can also modify these details if you are logged in with the require administrative privileges. This tool is useful for administrators (like typical Customer Service Representatives (CSRs)) for handling user queries.

NOTE: If user information is stored in LDAP, then you cannot change the user attributes.

- **Support for Password-Strength Checks for Credentials**

  You can now configure various password-strength parameters in WebFort. These parameters are checked during the create, reissue, and reset operations.

- **Support for Credential Auto-Unlock**

  WebFort also supports auto-unlocking of a credential after the configured time. The *auto-unlock* operation is performed when the user authenticates successfully after the configured time has elapsed.

- **Ability to Use One-Time Passwords (OTPs) Multiple Times**

  An OTP can now be used multiple times. As a result, an OTP can not only be used for a specified time interval, but also can be reused for pre-configured number of times.

- **Support for Credential Notes**

  WebFort now enables your application to maintain notes for all the supported native credentials. This allows applications to manage user- or credential-specific policies other than what WebFort supports.

- **Logging Enhancements**
  - **Audit Logging Enhancements**

    WebFort issuance and authentication audit logs have been enhanced to contain:

    - User identity
    - Credential details that include the type of the credential, strike count, status, usage count, validity start, validity end
    - Caller details, such as caller ID, Caller IP Address, WebFort SDK Protocol Version
    - Transaction result details, such as Response Code, Reason Code, Time taken to process the request
    - Transaction details that include Transaction ID, Session ID, Operation, Locale
    - Configuration details, such as Name and Version of each configuration used

- VAS Event details, such as Event ID, Module Name, Module Result, Transaction ID, Message

NOTE: VAS Event details are logged for every plug-in and callout that is configured.

- **File Logging Enhancements**

  These enhancements include:

  - The readability of Server log files has been improved significantly.
  - The logs are now "script-friendly."
  - Every transaction (receive, send, operation, response details, and processing time) is now logged unconditionally.
  - Complete non-sensitive request and response data is logged if the logging level is `DETAIL`.
  - Traces can be enabled, irrespective of the log level, to get more details of the transaction flow.

- **Support for Configuration Versioning**

  With this release, all WebFort configurations will be versioned. This will enable you to track all the configuration changes made by using the Administration Console.

- **Built-in LDAP Authentication Plug-In**

  WebFort now ships with a built-in plug-in that can perform LDAP username-password authentication.

  NOTE: You must explicitly configure a plug-in for a given organization.

- **Support for SAML Tokens**

  WebFort now provides the capability to return a SAML Assertion in response to successful authentications. SAML Assertion versions 2.0 and 1.1 are supported.

  Number of attributes to be returned as part of the SAML Assertion can be configured. These attributes are fetched from LDAP or database, depending on your configuration.

- **ASSP Enhancements**

  This release introduces:

  - Support for latest ASSP Web-Service interface.

- Support for ArcotID Client "inside" Adobe Acrobat(TM) or Adobe Reader(TM) versions 9.1 and later.
- Support for configuring SAML, authentication mechanism list, and related features at the organization level.

- **OpenSSL CA and ArcotID Domain Key Creation at Startup**

  The OpenSSL CA and ArcotID Domain Keys are now automatically created by the server when it starts up. This enables you to issue ArcotID and support ArcotID authentication without having to perform these additional tasks.

- **Enhanced APIs**

  WebFort APIs have been enhanced to support atomic issuance of multiple credentials. In addition:

  - WebFort allows an arbitrary number of additional input parameters to be exchanged between your calling application and the plug-in or callout.
  - Similarly, WebFort also allows an arbitrary number of additional output parameters to be exchanged between the plug-in or callout and your calling application.

- **Other SDK Enhancements**

  - **Support for Validations at the Server-End**

    Starting with this release, all validation tasks have been centralized to be performed by the Server. This makes SDKs of different flavors (Java or Web Services) and different versions more consistent and predictable in behavior. This also reduces the size of the SDKs and also makes the upgrade or migration to the newer versions of WebFort easy.

    IMPORTANT: To use this feature, all applications *must* use the new SDKs. Refer to Chapter 6, "Configuring Java SDKs and Web Services" for more information on backward compatibility support.

  - **Support for Connection Pooling and Failover in SDKs**

    WebFort Authentication and Issuance Java SDKs now provide the ability to build a pool of connections to the server, such that the transaction-time cost of creating a connection can be avoided.

    Also, the Java SDKs now provide the capability to seamlessly failover to other Server instances if the current instance is unavailable.

- **Protected Web Services**

  Starting with this release, Web services are protected from rogue requests through authentication and authorization of all Web service requests. As a result, all requests to WebFort Web services are authenticated for valid credentials. After successful authentication, all requests are then validated for appropriate privileges to access the Web services. This is done using the `webfortserver` tool, see Chapter 9, "Tools for System Administrators" in *Arcot WebFort 6.0 Administration Guide*.

- **Sample Application Improvements**

  Following enhancements have been made to the Sample Application:

  - Code showcases the new APIs.
  - Code is moved from Java files to JSP for easier modification and use by developers, if they choose to do so.
  - A new Setup screen is provided to configure WebFort Server connection information. This screen eliminates the need of changing the configuration file on the system where the Sample Application is deployed.
  - The GUI changes ensure that all the feature links of the Sample Application are always visible.
  - ArcotID Client configuration can be selected and preserved for a session, so that you can explore all ArcotID flows for a client configuration.
  - Links for user name-password issuance and authentication have been introduced.
  - Details of all credentials can be retrieved by using the Fetch operation.

- **Documentation Changes**

  This release is shipped with two new guides, *Arcot WebFort 6.0 Java Developer's Guide* and *Arcot WebFort 6.0 Business Logic Extension Guide*. The *Arcot WebFort 6.0 Administration Guide* has also been improved to reflect the changes made in the new Administration Console.

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 briefly outlines the steps for deploying 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. 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.
4. 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.
5. Deploy the Web-based applications. Refer to the following:
   - "Deploying Web Applications" for single-system deployment.
   - "Deploying Web Applications" for distributed-system deployment.
6. Log in to Administration Console and bootstrap the system. Refer to the following:
   - "Bootstrapping the System" for single-system deployment.
   - "Bootstrapping the System" for distributed-system deployment.

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.

WebFort Server is the primary component for installation. Apart form WebFort Server, Java SDKs and Web Services are provided to integrate with your application.

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

The component diagrams discussed in this chapter are for Java SDKs, the Web services deployment is also done in a similar fashion. Use the WSDLs for authentication and issuance Web services and generate the client by using the software of your choice.

> **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 on a Single System

In a single-system deployment, all components of WebFort and the Web applications 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.

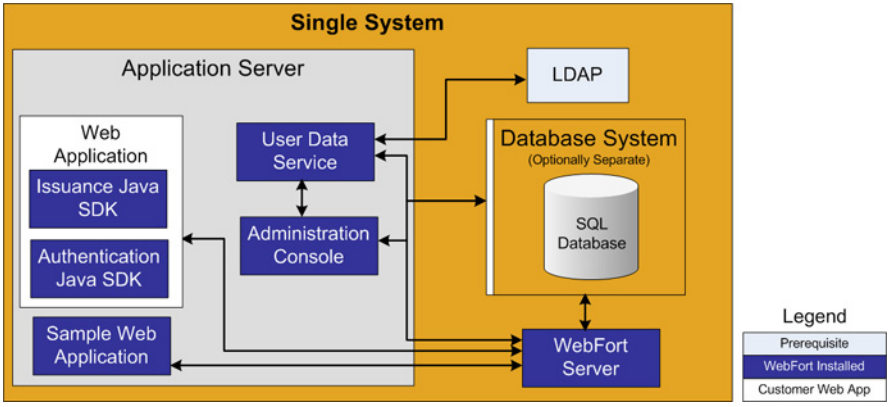
If you plan to perform a single-system deployment, then you must make the following decisions:

Decision: Install a database server on the system which has WebFort Server or use an existing database on a separate system.

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

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

Figure 2-1 Deploying WebFort Components on Single System



Deploying on Distributed Systems

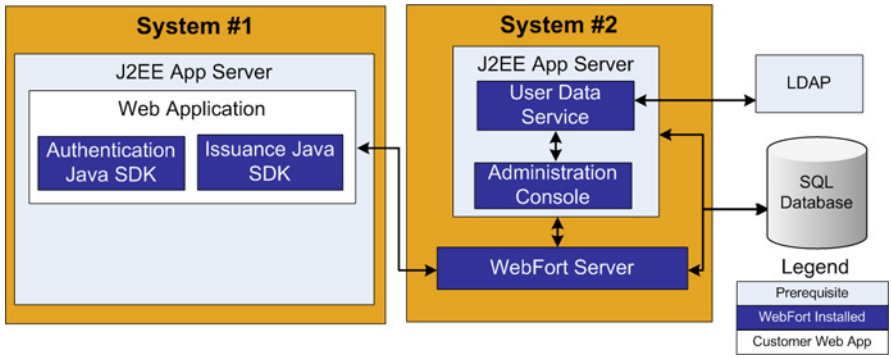
In a distributed-system deployment, WebFort components are installed on different systems. This type of deployment increases the security and performance. This model is typically used for production deployments or staging environments.

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.

Deploying Java SDKs on a Single Application

The following figure illustrates deployment of WebFort using Java SDKs on a single application. For high-availability deployment, you can use this approach and deploy on multiple systems to ensure operational continuity.

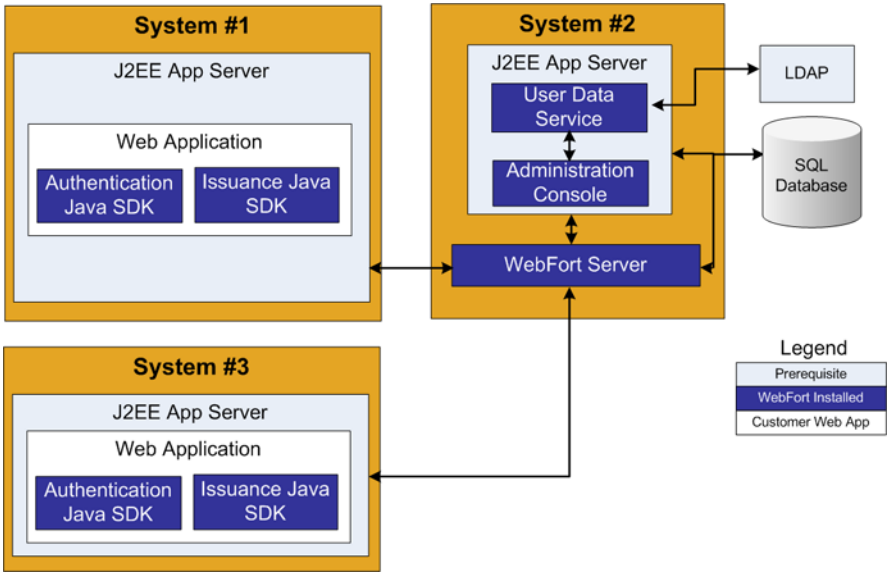
Figure 2-2 Java SDKs on Single System



Deploying Java SDKs on Multiple Applications

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

Figure 2-3 Java SDKs on Multiple Systems



Chapter 3

Preparing for Installation

Before installing WebFort, ensure that your computer meets the requirements described in this chapter. The chapter also provides the database information that you have to collect before installing WebFort. It contains the following sections:

- System Requirements
- Installation Checklists

System Requirements

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

Hardware Requirements

The hardware requirements mentioned here are for WebFort (only) and does not include the hardware that is required for the prerequisite software such as database or application server.

- RAM: 1 GB
- Hard Drive Space: 10 GB

Software Requirements

This sub-section provides the list of minimal software required to install WebFort:

> **NOTE:** For all the third-party software mentioned in the following table, it is assumed that the higher versions are compatible with the specified supported version.

Table 3-1 Minimum Software Requirements

Software Type	Version
Operating System	Windows Server 2003 Enterprise Edition SP2
Database	The following database servers are supported: • Microsoft SQL Server 2005, Standard Edition (SP2) or higher • Oracle 10g or higher
Directory Server	The following directory servers are supported: • Windows Active Directory 2003 • SunOne Directory Server 5.2 and 6.1

Table 3-1 Minimum Software Requirements

Software Type	Version
Application Server	The following application servers are supported: • Apache Tomcat 5.5.23 or higher (http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.23/bin/) • IBM WebSphere 6.1 or higher • BEA WebLogic 10 or higher
JDK	The JDK version that is compatible with your application server.

Installation Checklists

Pre-Installation Checklist

Arcot recommends that you fill in this checklist before you proceed with the installation and setup of WebFort.

Table 3-2 Pre-Installation Checklist

Your Information	Example Entry	Your Entry
HARDWARE		
Processor	Pentium® 4 GHz	
RAM	2 GB	
Disk Space	20 GB	
SOFTWARE		
Operating System	Windows Server 2003	
Distribution	Enterprise Edition	
Service Pack (or Patch)	SP2	
DATABASE		
Type	Oracle	
DSN Name	webfort	
Host Name (or Server)	webfort	
Port (*Oracle Databases Only*)	1521	
Service ID (*Oracle Databases Only*)	ocsdb1	
User Name	dbadmin	
Password	password1234!	
Configured Privileges:		
CREATE TABLE	✓	
CREATE INDEX	✓	
CREATE PROCEDURE	✓	
REFERENCES	✓	

Table 3-2 Pre-Installation Checklist

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

Post-Installation Checklist

Arcot recommends that you fill in this checklist with the installation and setup information for WebFort. You will need this information for various administrative tasks that you will do.

Table 3-3 Installation Checklist

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

Chapter 4

Deploying WebFort on a Single System

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

The following list provides 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".
- Deploy Web-based applications in the application server, see "Deploying Web Applications".
- Verify the installation, see "Verifying the Installation".
- Log in to Administration Console as the Master Administrator to bootstrap the system. See "Logging In to Administration Console".

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.

Installing WebFort

This section guides you through installing WebFort for a single-system deployment. You must ensure that the account that you plan to use for installation belongs to the Administrators group. This is because some critical steps in the installation, such as DSN creation and configuration, and WebFort service creation, will not go through successfully, though the installation might complete without any errors.

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".

> **NOTE:** Before running the WebFort installer, ensure that you have set `<JAVA_HOME>/bin` in the `PATH` environment variable, else `arcotadmin.war` file generation might fail.

Perform the following steps to install WebFort and related components:

1. Locate the WebFort installer `Arcot-WebFort-6.0-Windows-Installer.exe` file.
2. Double-click the installer `Arcot-WebFort-6.0-Windows-Installer.exe`.

   The Welcome screen appears.
3. Click the **Next** button to proceed.

   The License Agreement screen appears.
4. Read the License Agreement. Select the **I accept the terms in the license agreement** option, and click the **Next** button to accept the agreement.

   The Installation Location screen appears.
5. By default, WebFort is installed in a folder called `Arcot Systems` in `<%SystemDrive%>\Program Files\`. To change the install location click the **Choose** button and select a folder. To restore the default folder, click the **Restore Default Folder** button.
6. Click **Next** button to continue with the installation.

   The Installation Type screen appears.
7. Select the **Complete** option to install all components and click **Next**.

   The Database Type screen appears.

8. Select the database type **Microsoft SQL Server** or **Oracle** and click **Next** to proceed.

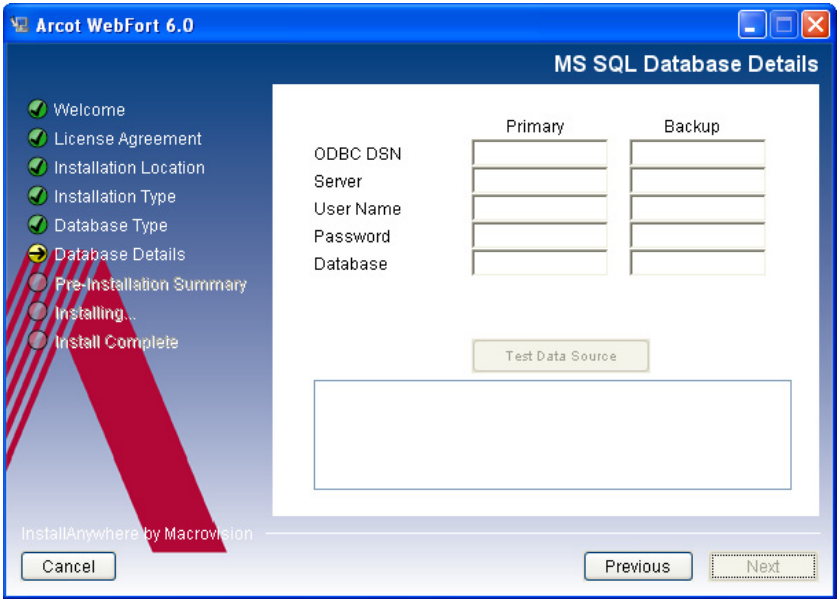
   Depending on the Database you selected, the corresponding Database Details screen appears.

   Go to Step a if you selected Microsoft SQL or Step b if you selected Oracle.

   a. Microsoft SQL Database Details

      The following figure displays the Microsoft SQL Database details required by WebFort.

Figure 4-1 MS SQL Database Details



Perform the following tasks for MS SQL database access:

i. Enter the required information, see the following table for field details.

Table 4-1 Microsoft SQL Server Details

Field	Description
ODBC DSN	WebFort Server uses the ODBC DSN to connect to the Arcot database. The recommended value to enter is *arcotdsn*.

Table 4-1 Microsoft SQL Server Details

Field	Description
Server	The host name or IP address of the database server. If SQL server is deployed in **Named Instance** mode, then you must also enter a slash "\" followed by the instance name, refer to vendor documentation for more information on this. **Default Instance** **Syntax**: <*Server Name*> **Example**: demodatabase **Named instance** **Syntax**: <*Server Name*>\<*instance name*> **Example**: demodatabase\instance1
User Name	The User Name that WebFort uses to access the database (SQL Server refers to this as *login)*. This name is specified by the database administrator. **NOTE:** The User Name for the Primary and Backup DSN must be different.
Password	The password that WebFort uses to access the database. This password is specified by the database administrator.
Database	The name of the database that WebFort will access.

i. Test for successful database connection by clicking **Test Data Source**.

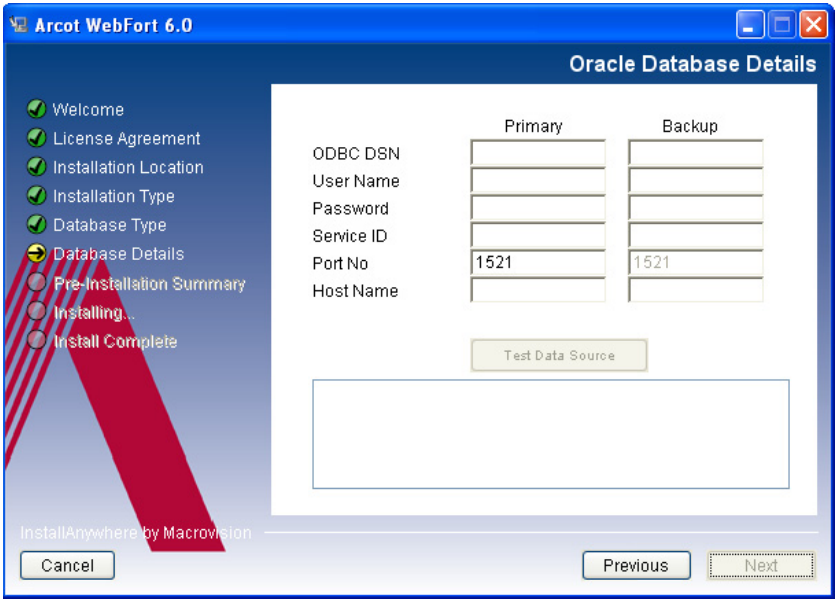
ii. After completing the test, click **Next** to proceed.

iii. Go to **Step 9**.

b. Oracle Database Details

The following figure displays the Oracle Database details required by WebFort.

Figure 4-2 Oracle Database Details



Perform the following tasks for Oracle database access:

i. Enter the required information, see the following table for field details.

Table 4-2 Oracle Database Details

Field	Description
ODBC DSN	WebFort Server uses the ODBC DSN to connect to the Arcot database. The recommended value to enter is *arcotdsn*.
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 must 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 on which the database server listens to the incoming requests.

Table 4-2 Oracle Database Details

Field	Description
Host Name	The host name or the IP address of the computer where the Oracle server is available. **Syntax**: <*Server Name*> **Example**: demodatabase

ii. Test for successful database connection by clicking **Test Data Source**.

iii. After completing the test, click **Next** to proceed.

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

9. Select **Yes, restart my system** to restart the system after completing the installation process.

10. Click **Done** to exit the installation wizard.

NOTE: To view the installation activity, refer to the log file `Arcot_WebFort_InstallLog.log` at `<install_location>\Arcot Systems\logs\.`

Post-Installation Tasks

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

1. Running Database Scripts
2. Deploying Web Applications
3. Logging In to Administration Console
4. Bootstrapping the System
5. Starting WebFort Server
6. Verifying the Installation
7. Deploying Sample Application

> **NOTE:** After completing these post-installation tasks, perform the Java SDKs and Web Services configuration as discussed in Chapter 6, "Configuring Java SDKs and Web Services".

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 type. The default location is:

For Oracle: `<install_location>\Arcot Systems\dbscripts\oracle`

For MS SQL: `<install_location>\Arcot Systems\dbscripts\mssql`

2. Run the *scripts in the following order* by using the database vendor tools:
   a. `arcot-db-config-for-common-1.0.sql`
   b. `arcot-db-config-for-webfort-6.0.sql`

> **NOTE:** If you encounter any error while executing the scripts, then check with your database administrator whether you have the required privileges.

Deploying Web Applications

This section describes the steps to copy the files that are required by User Data Service and Administration Console, and deploy the WAR files of these applications.

- Preparing Your Application Server
- (Optional) Creating Enterprise Archive File
- Starting WebFort Server
- Deploying Administration Console

Preparing Your Application Server

This sub-section provides the steps to copy the Arcot files `ArcotAccessKeyProvider.dll` and `arcot-crypto-util.jar` files for the following application servers:

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

The `ArcotAccessKeyProvider.dll` library file is available at the following location:
`<install_location>\Arcot Systems\java\ext\win\<32 or 64 bit>\`

The `arcot-crypto-util.jar` file is available at the following location:
`<install_location>\Arcot Systems\java\ext\`

Apache Tomcat

Perform the following steps to copy the Arcot files:

1. Copy the `ArcotAccessKeyProvider.dll` file to `<JAVA_HOME>\jre\bin` directory.
2. Copy the `arcot-crypto-util.jar` file to `<JAVA_HOME>\jre\lib\ext` directory.
3. Restart the application server.

IBM WebSphere

Perform the following steps to copy the Arcot files on WebSphere 6.1:

1. Log into WebSphere Administration Console.
2. Click **Environment**, and then click **Shared Libraries**.

a. From the **Scope** drop-down, select a valid visibility scope. The scope must include the target server/node on which the application is deployed.

b. Click **New**.

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

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

e. Enter the JNI library path. This path must point to the location where the `ArcotAccessKeyProvider.dll` file is present.

3. Configure server-level class loaders.

a. Click **Servers**, and then click **Application Servers.**

b. Under **Application Servers** access the settings page of the server for which the configuration are performed.

c. Click **Java and Process Management**, and then click **Class Loader**.

d. Click **New**. Select default **Classes loaded with parent class loader first** and click **OK.**

e. Click the auto-generated **Class Loader ID**.

f. In the class loader **Configuration** page, click **Shared Library References**.

g. Click **Add**, select ArcotJNI and then click **Apply**.

h. Save the changes made.

4. Copy `ArcotAccessKeyProvider.dll` file to `<JAVA_HOME_used by WebSphere>\jre\bin` folder.

5. Restart WebSphere.

BEA WebLogic

Perform the following steps to copy the Arcot files:

1. Copy `ArcotAccessKeyProvider.dll` to WebLogic's `<JAVA_HOME used by WebLogic instance>\jre\bin`.

2. Copy `arcot-crypto-util.jar` to WebLogic's `<JAVA_HOME used by WebLogic instance>\jre\lib\ext`.

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

3. Login to WebLogic Admin Console.
4. Navigate to **Deployments**.
5. Enable the **Lock and Edit** option.
6. Click **Install** and navigate to the directory that contains the `arcot-crypto-util.jar` file.
7. Click **Next**.

   The Application Installation Assistant screen appears.
8. Click **Next**.

   The Summary page appears.
9. Click **Finish**.
10. Activate the changes.
11. Restart the WebLogic server.

(Optional) Creating Enterprise Archive File

By default, WebFort provides Web ARchive (WAR) files to deploy Administration Console and User Data Service (UDS). You can also change the format of these files to Enterprise ARchive (EAR) and then deploy the EAR files.

Generating Separate EAR Files

Perform the following steps to create EAR file for Administration Console or User Data Service:

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

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

   The above command generates the EAR file and it is available at `<install_location>\Arcot Systems\java\webapps`.

Generating a Single EAR File

Perform the following steps to create a single EAR file containing Administration Console and UDS Web archives:

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

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

   The above command generates the EAR file and is available at `<install_location>\Arcot Systems\java\webapps`.

Deploying User Data Service

You need the file `arcotuds.war` to deploy the User Data Service (UDS).

To deploy User Data Service:

1. Install `arcotuds.war` available at `<install_location>\Arcot Systems\java\webapps` 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. (**For WebSphere Only**) Configure to reload the UDS class when the application files are updated.
   a. Navigate to **Application** > **Enterprise Applications** and access the UDS settings page.
   b. Under **Class loader order**, select the **Classes loaded with local class loader first** (**parent last**) option.
   c. Under **WAR class loader policy**, select the **Single class loader for application**.
   d. Click **Apply** to save the changes made.
3. Perform the following steps to verify if UDS started correctly:
   a. Navigate to the following location:

      `<install_location>\Arcot Systems\logs`

   b. Open the `arcotuds.log` file in any editor and locate the following lines:
      - `UDS Initialized successfully`
      - `Starting Arcot UDS Version 1.0`

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

Deploying Administration Console

You need the file `arcotadmin.war` to deploy the WebFort Administration Console.

To deploy Administration Console:

1. Install `arcotadmin.war` available at `<install_location>\Arcot Systems\java\webapps` 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. Perform the following steps to verify if the Administration Console started correctly:

   a. Navigate to the following location:

      `<install_location>\Arcot Systems\logs`

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

      - `Arcot Administration Console v1.0`
      - `Servlet 'arcotadmin' configured successfully`

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

Logging In to Administration Console

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

To log in to Administration Console:

1. Start Administration Console in a Web browser window, by using the following URL:

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

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

2. Log in to Administration Console as a Master Administrator with the default Master Administrator account credentials. The credentials are:
   - **User Name**: masteradmin
   - **Password**: master1234!

Bootstrapping the System

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

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

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

Before you proceed with **Performing the Bootstrapping Tasks**, you must understand the following related concepts:

- **User Data Service (UDS)**
- **Default Organization**

User Data Service (UDS)

User Data Service (UDS) enables access to the third-party data repositories (LDAP directory servers) deployed by your organization. As a result, it enables WebFort Server and the Administration Console to seamlessly access your existing data. If the LDAP directory server is not configured, then it accesses the WebFort database to read the user information. See **Step 3 on page 44** in the bootstrapping steps to know about the parameters that must be set to connect UDS to other WebFort components.

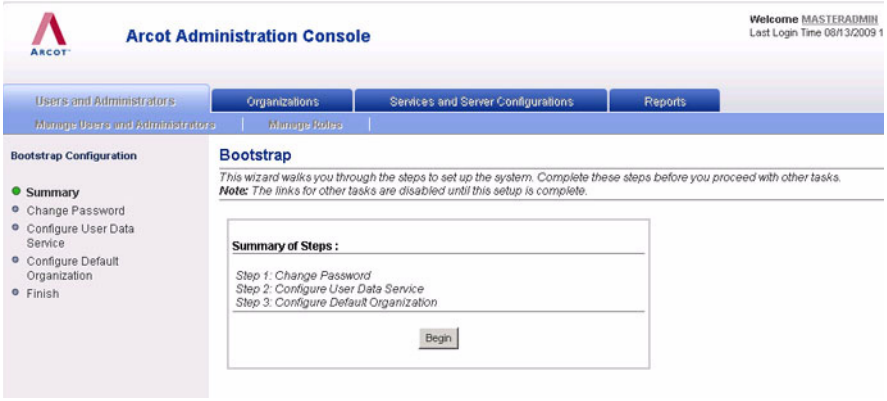
Default Organization

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

Performing the Bootstrapping Tasks

When you first log in to the Administration Console as the Master Administrator (MA), the Summary screen for the Bootstrap wizard screen (**Figure 4-3**) appears.

Figure 4-3 Bootstrap Wizard: Summary Screen



To bootstrap the system using the wizard:

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

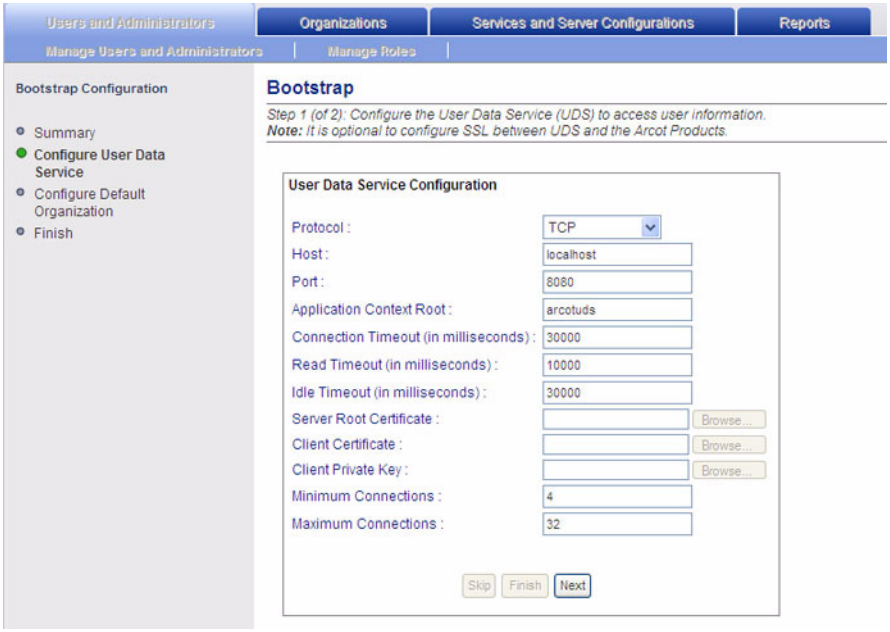
   The Change Password screen, as shown in Figure 4-4, appears.

Figure 4-4 Bootstrap Wizard: Change Password Screen

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

   The Configure User Data Service screen, as shown in Figure 4-5, appears.

Figure 4-5 Bootstrap Wizard: Configure User Data Service Screen



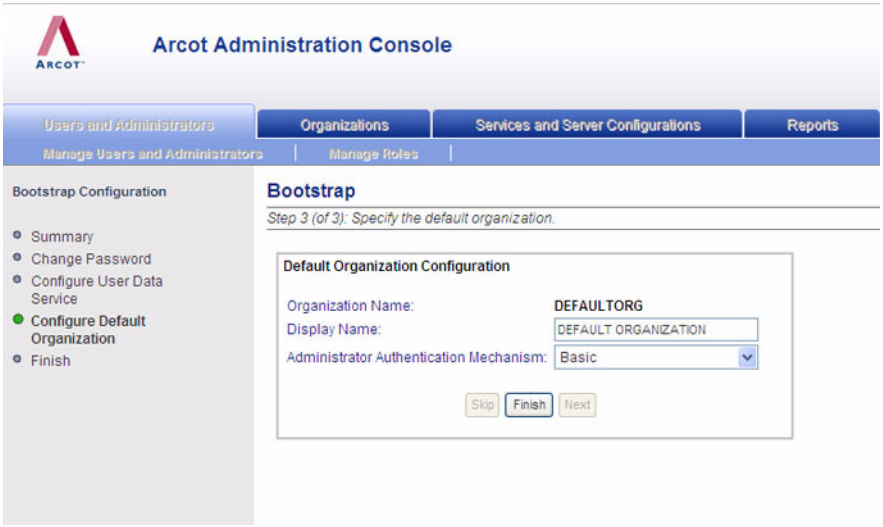
3. Specify the parameters listed in Table 4-3 to configure UDS:

Table 4-3 UDS Configuration Parameters

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

The Configure Default Organization screen, shown in Figure 4-6, appears.

Figure 4-6 Bootstrap Wizard: Configure Default Organization Screen



4. Specify the following parameters for the Default Organization:

   - **Display Name:** The descriptive name of the organization. This name appears on all other Administration Console pages and reports.
   - **Authentication Mechanism:** The mechanism that is used to authenticate administrators belonging to the Default Organization. Administration Console supports 2 types of authentication methods for the administrators to log in:
     - **Basic User Password**

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

       If you select the **WebFort User Password** option here, then the credentials are issued and authenticated by the WebFort Server. Refer to *Arcot WebFort 6.0 Administration Guide* for more information on how to do this.

   The Administration Console initialization is completed, as indicated in the Finish screen (Figure 4-7).

Figure 4-7 Bootstrap Wizard: Finish Screen

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

Starting WebFort Server

Perform the following steps to start WebFort Server:

1. On the task bar, click the **Start** button.
2. Click **Settings**, and then point to **Control Panel**, **Administrative Tools**, and **Services.**
3. Select **Arcot WebFort Authentication Service**.
4. Click the **Start** button to start the service.

NOTE: If you want to stop the server, then click the **Stop** button.

Verifying the Installation

You can verify whether the WebFort Server and the Web applications have started successfully by:

- Using Log files
- Using arwfclient
- Checking the Ports

Using Log files

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

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs`

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

   - `INSTANCE_VER.....: [6.0]`
   - `Arcot WebFort Authentication Service READY`

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

Using arwfclient

The `arwfclient` tool enables you to check the version of WebFort you have installed. Refer to *Arcot WebFort 6.0 Administration Guide* for more information on this tool.

Perform the following steps to check the WebFort version:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\bin`

2. Execute **`arwfclient.exe`** with the following option:

   ```
   arwfclient ver
   ```

   The **`webfort-ver-<dd>-<mmm>-<yy>.txt`** file is created in the `<install_location>\Arcot Systems\logs folder.`

3. Open this file and check whether the version of library files is `6.0`.

Checking the Ports

Perform the following steps to verify if the WebFort Server is listening to different protocols on the default ports:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs`

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

   ```
   PROTOCOLNAME : [Administration-WS]
   ```

```
PORTNO : 9745

PROTOCOLID : [Authentication-ASSP]
PORTNO : 9741

PROTOCOLID : [Authentication-Native]
PORTNO : 9742

PROTOCOLID : [Authentication-RADIUS]
PORTNO : 1812

PROTOCOLID : [Authentication-WS]
PORTNO : 9744
```

NOTE: Refer to **Appendix D, "Default Port Numbers and URLs"** for information on default ports and protocols.

Deploying Sample Application

Sample Application can be used for testing WebFort or as a code sample for integrating ArcotID and other authentication methods into existing Web applications.

To deploy Sample Application:

1. Deploy the `webfort-6.0-sample-application.war` file from the following location:

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

2. Access the Sample Application using the following URL:

   `http://<host>:<port>/webfort-6.0-sample-application/`

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 list provides a quick overview of the process:

- Execute the WebFort 6.0 installer to add WebFort Server and Administration Console to your file system and configure them to access your SQL database. See **"Installing on First System"** for install instructions.
- Execute the database scripts to create schema and database tables, see **"Running Database Scripts"**.
- Deploy Web-based applications in the application server, see **"Deploying Web Applications"**.
- Log in to Administration Console as the Master Administrator to bootstrap the system. 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.
- Deploy Sample Application, 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.

Installing on First System

This section guides you through the steps for installing WebFort for your distributed-system deployment or high-availability deployment. You must ensure that the account that you plan to use for installation belongs to the Administrators group. This is because some critical steps in the installation, such as DSN creation and configuration, and WebFort service creation, will not go through successfully, though the installation might complete without any errors.

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".

> **NOTE:** Before running the WebFort installer, ensure that you have set `<JAVA_HOME>/bin` in the `PATH` environment variable, else `arcotadmin.war` file generation might fail.

Perform the following steps to install WebFort and related components:

1. Locate the WebFort installer `Arcot-WebFort-6.0-Windows-Installer.exe` file.
2. Double-click the installer `Arcot-WebFort-6.0-Windows-Installer.exe`.

   The Welcome screen appears. It might take some time for this screen to appear.
3. Click the **Next** button to proceed.

   The License Agreement screen appears.
4. Read the License Agreement. Select the **I accept the terms in the license agreement** option, and click the **Next** button to accept the agreement.

   The Installation Location screen appears.
5. By default, WebFort is installed in a folder called `Arcot Systems` in `<%SystemDrive%>\Program Files\`. To change the install location click the **Choose** button and select a folder. To restore the default folder, click the **Restore Default Folder** button.
6. Click **Next** button to continue with the installation.

   The Choose Type of Installation screen appears.
7. Select the **Custom** option to install the selected components and click **Next**.

   The Component Selection screen appears. This screen displays all the components provided by WebFort.

8. Select WebFort Server, Administration Console, and User Data Service.
9. After you have selected all the desired components for installation, click **Next**.

   The Database Type screen appears.
10. Select the database type **Microsoft SQL Server** or **Oracle** and click **Next** to proceed.

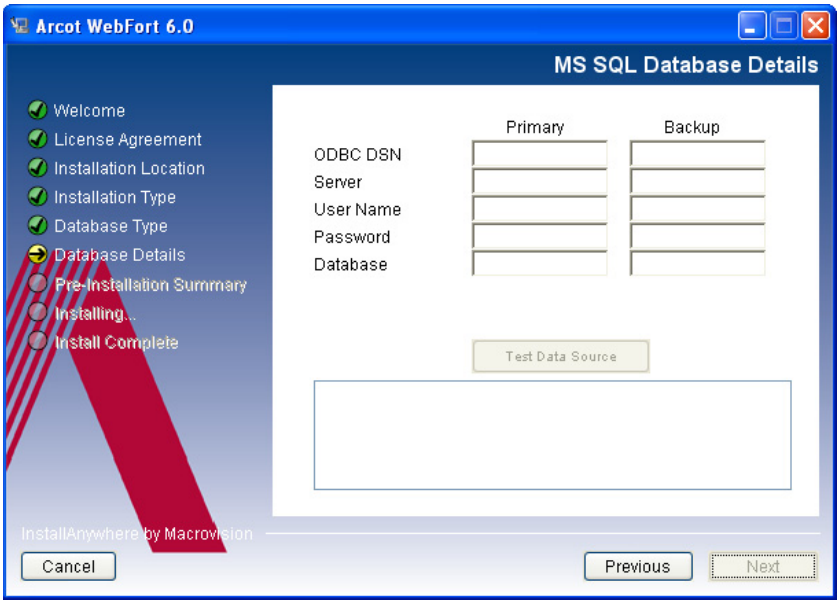
    Depending on the Database you selected, the corresponding Database Details screen appears.

    Go to Step a if you selected Microsoft SQL or Step b if you selected Oracle.

    a. Microsoft SQL Database Details

       The following figure displays the Microsoft SQL Database details required by WebFort.

Figure 5-1 MS SQL Database Details



Perform the following tasks for MS SQL database access:

i. Enter the required information, see the following table for field details.

Table 5-1 Parameters for Microsoft SQL Server Access

Field	Description
ODBC DSN	WebFort Server uses the ODBC DSN to connect to the Arcot database. The recommended value to enter is *arcotdsn.*
Server	The host name or IP address of the database server. If SQL server is deployed in **Named Instance** mode, then you must also enter a slash "\" followed by the instance name, refer to vendor documentation for more information on this. **Default Instance** **Syntax**: <*Server Name*> **Example**: demodatabase **Named instance** **Syntax**: <*Server Name*>\<*instance name*> **Example**: demodatabase\instance1
User Name	The User Name that WebFort uses to access the database (SQL Server refers to this as *login)*. This name is specified by the database administrator. **NOTE:** The User Name for the Primary and Backup DSN must be different.
Password	The password that WebFort uses to access the database. This password is specified by the database administrator.
Database	The name of the database that WebFort will access.

ii. Test for successful database connection by clicking **Test Data Source**.

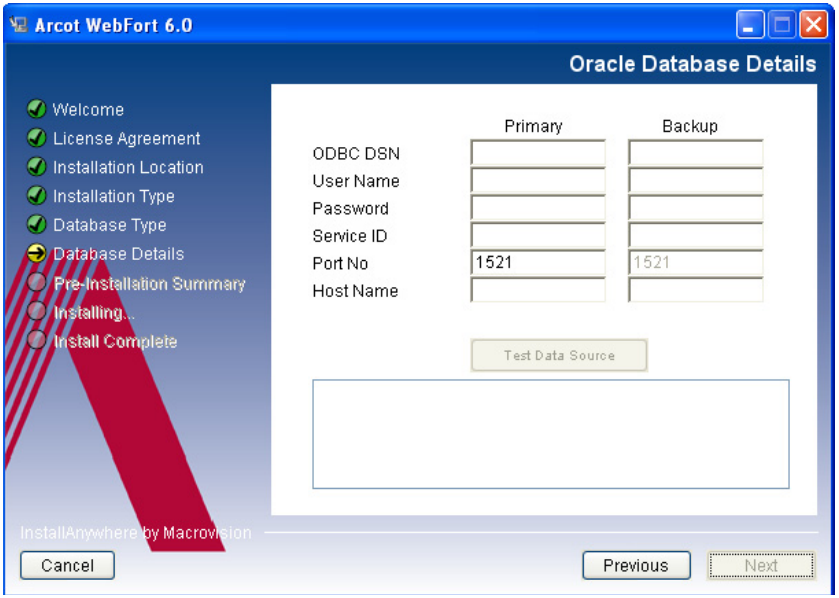
iii. After completing the test, click **Next** to proceed.

iv. Go to Step 11.

b. Oracle Database Details

The following figure displays the Oracle SQL Database details required by WebFort.

Figure 5-2 Oracle Database Details



Perform the following tasks for Oracle database access:

i. Enter the required information, see the following table for field details.

Table 5-2 Parameters for Oracle Database Access

Field	Description
ODBC DSN	WebFort Server uses the ODBC DSN to connect to the Arcot database. The recommended value to enter is *arcotdsn*.
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 on which the database server listens to the incoming requests.

Table 5-2 Parameters for Oracle Database Access

Field	Description
Host Name	The host name or the IP address of the computer where the Oracle server is available. **Syntax**: <*Host Name* or *IP address*> **Example**: demodatabase

ii. Test for successful database connection by clicking **Test Data Source**.

iii. After completing the test, click **Next** to proceed.

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

11. If you want to change any of the installation settings, then click the **Previous** button or click the **Install** button to proceed with the installation.

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

12. Select **Yes, restart my system** to restart the system after completing the installation process.

13. Click **Done** to exit the installation wizard.

NOTE: To view the installation activity, refer to the log file `Arcot_WebFort_InstallLog.log` at `<install_location>\Arcot Systems\logs\.`

Post-Installation Tasks for First System

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

1. Running Database Scripts
2. Deploying Web Applications
3. Logging In to Administration Console
4. Bootstrapping the System
5. Starting WebFort Server
6. Verifying the Installation

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 type. The default location is:

For Oracle: `<install_location>\Arcot Systems\dbscripts\oracle`

For MS SQL: `<install_location>\Arcot Systems\dbscripts\mssql`

2. Run the *scripts in the following order* by using the database vendor tools:
   a. `arcot-db-config-for-common-1.0.sql`
   b. `arcot-db-config-for-webfort-6.0.sql`

NOTE: If you encounter any error while executing the scripts, then check with your database administrator whether you have the required privileges.

Deploying Web Applications

This section describes the steps to copy files that are required by User Data Service and Administration Console, and deploy the WAR files of these applications.

- Preparing Your Application Server

- (Optional) Creating Enterprise Archive File
- Deploying User Data Service
- Deploying Administration Console

Preparing Your Application Server

This sub-section provides the steps to copy the Arcot files `ArcotAccessKeyProvider.dll` and `arcot-crypto-util.jar` files for the following application servers.

- Apache Tomcat
- WebSphere
- WebLogic

The `ArcotAccessKeyProvider.dll` library file is available at the following location:
`<install_location>\Arcot Systems\java\ext\Win\<32 or 64 bit>`

The `arcot-crypto-util.jar` library file is available at the following location:
`<install_location>\Arcot Systems\java\ext\`

Apache Tomcat

Perform the following steps to copy the Arcot files:

1. Copy `ArcotAccessKeyProvider.dll` to `<JAVA_HOME>\jre\bin` directory.
2. Copy `arcot-crypto-util.jar` to `<JAVA_HOME>\jre\lib\ext` directory.
3. Restart Tomcat.

WebSphere

Perform the following steps to copy the Arcot files on WebSphere 6.1:

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

e. Enter the JNI library path. This path must point to the location where the `ArcotAccessKeyProvider.dll` file is present.

3. Configure server-level class loaders.

   a. Click **Servers**, and then click **Application Servers.**

   b. Under **Application Servers** access the settings page of the server for which the configuration are performed.

   c. Click **Java and Process Management**, and then click **Class Loader**.

   d. Click **New**. Select default **Classes loaded with parent class loader first** and click **OK.**

   e. Click the auto-generated **Class Loader ID**.

   f. In the class loader **Configuration** page, click **Shared Library References**.

   g. Click **Add**, select ArcotJNI and then click **Apply**.

   h. Save the changes made.

4. Copy `ArcotAccessKeyProvider.dll` file to `<JAVA_HOME_used by WebSphere>\jre\bin` folder.

5. Restart WebSphere.

WebLogic

Perform the following steps to copy the Arcot files:

1. Copy `ArcotAccessKeyProvider.dll` to WebLogic's `<JAVA_HOME used by WebLogic instance>\jre\bin`.

2. Copy `arcot-crypto-util.jar` to WebLogic's `<JAVA_HOME used by WebLogic instance>\jre\lib\ext`.

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

3. Login to WebLogic Admin Console.

4. Navigate to **Deployments**.

5. Enable the **Lock and Edit** option.

6. Click **Install** and navigate to the directory that contains the `arcot-crypto-util.jar` file.

7. Click **Next**.

The Application Installation Assistant screen appears.

8. Click **Next**.

   The Summary page appears.

9. Click **Finish**.

10. Activate the changes.

11. Restart the WebLogic server.

(Optional) Creating Enterprise Archive File

By default, WebFort provides Web ARchive (WAR) files to deploy Administration Console and User Data Service (UDS). You can also change the format of these files to Enterprise ARchive (EAR) and then deploy the EAR files.

Generating Separate EAR Files

Perform the following steps to create EAR file for Administration Console or User Data Service:

1. Navigate to `<install_location>\Arcot Systems\tools\bundlemanager` directory.

2. Run the `bundlemanager` tool to create the EAR file by using the following command:

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

   The above command generates the EAR file and it is available at `<install_location>\Arcot Systems\java\webapps`.

Generating a Combined EAR File

Perform the following steps to create a single EAR file containing Administration Console and UDS Web archives:

1. Navigate to `<install_location>\Arcot Systems\tools\bundlemanager` directory.

2. Run the `bundlemanager` tool to create the EAR file by using the following command:

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

   The above command generates the EAR file and is available at `<install_location>\Arcot Systems\java\webapps`.

Deploying User Data Service

You need the file `arcotuds.war` to deploy the User Data Service (UDS).

To deploy User Data Service:

1. Install `arcotuds.war` available at `<install_location>\Arcot Systems\java\webapps` 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. (**For WebSphere Only**) Configure to reload the UDS class when the application files are updated.

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

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

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

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

3. Verify if UDS started correctly:

   a. Navigate to the following location:

      `<install_location>\Arcot Systems\logs`

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

      - `UDS Initialized successfully`
      - `Starting Arcot UDS Version 1.0`

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

Deploying Administration Console

You need the file `arcotadmin.war` to deploy the WebFort Administration Console.

To deploy Administration Console:

1. Install `arcotadmin.war` available at `<install_location>\Arcot Systems\java\webapps` 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. Verify if the Administration Console started correctly:

   a. Navigate to the following location:

   `<install_location>\Arcot Systems\logs`

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

   - `Arcot Administration Console v1.0`
   - `Servlet 'arcotadmin' configured successfully`

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

Logging In to Administration Console

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

To log in to Administration Console:

1. Start Administration Console in a Web browser window, by using the following URL:

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

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

2. Log in to Administration Console as a Master Administrator with the default Master Administrator account credentials. The credentials are:

   - **User Name**: masteradmin
   - **Password**: master1234!

Bootstrapping the System

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

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

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

Before you proceed with **Performing the Bootstrapping Tasks**, you must understand the following related concepts:

- **User Data Service (UDS)**
- **Default Organization**

User Data Service (UDS)

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

Default Organization

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

Performing the Bootstrapping Tasks

When you first log in to the Administration Console as the Master Administrator (MA), the Summary screen for the Bootstrap wizard screen (**Figure 5-3**) appears.

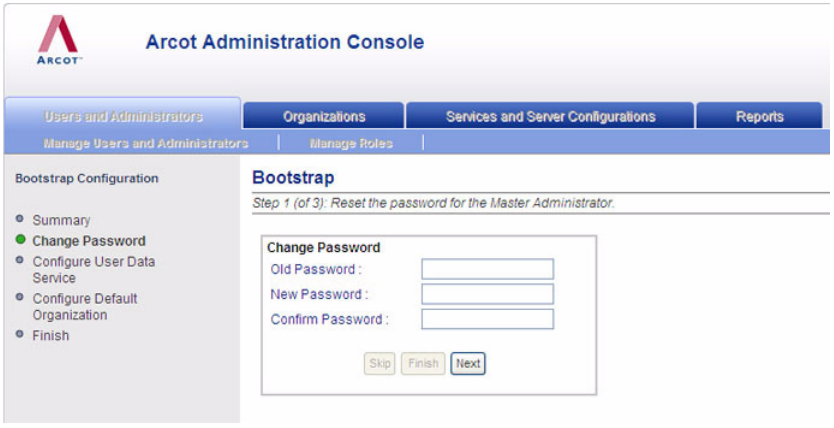
Figure 5-3 Bootstrap Wizard: Summary Screen

To bootstrap the system using the wizard:

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

   The Change Password screen, as shown in Figure 5-4, appears.

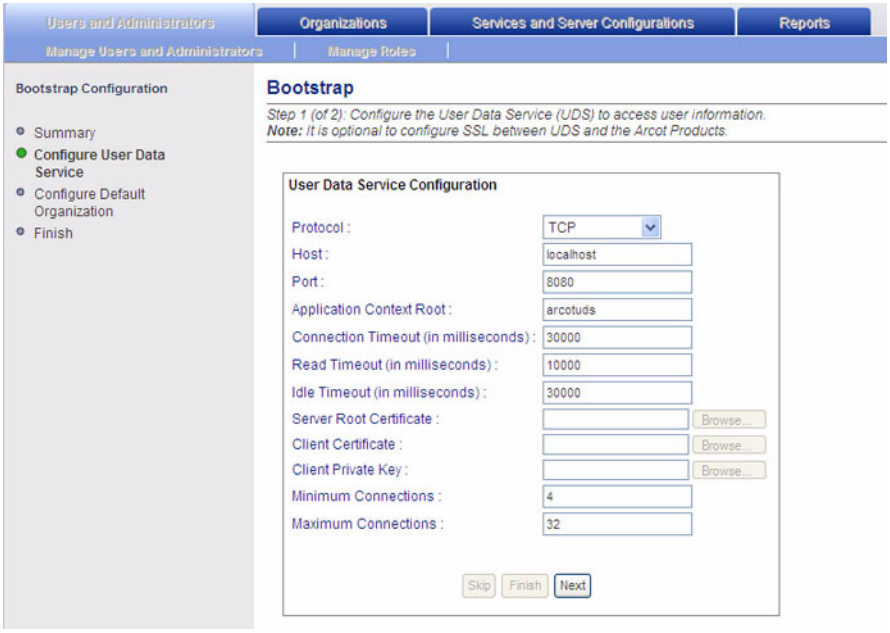
Figure 5-4 Bootstrap Wizard: Change Password Screen



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

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

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



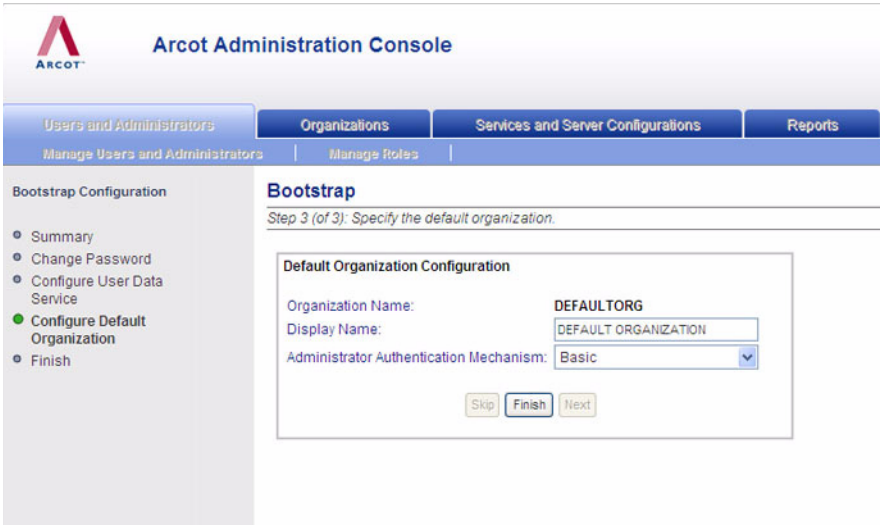
3. Specify the parameters listed in Table 5-3 to configure UDS:

Table 5-3 UDS Configuration Parameters

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

The Configure Default Organization screen, shown in Figure 5-6, appears.

Figure 5-6 Bootstrap Wizard: Configure Default Organization Screen



4. Specify the following parameters for the Default Organization:

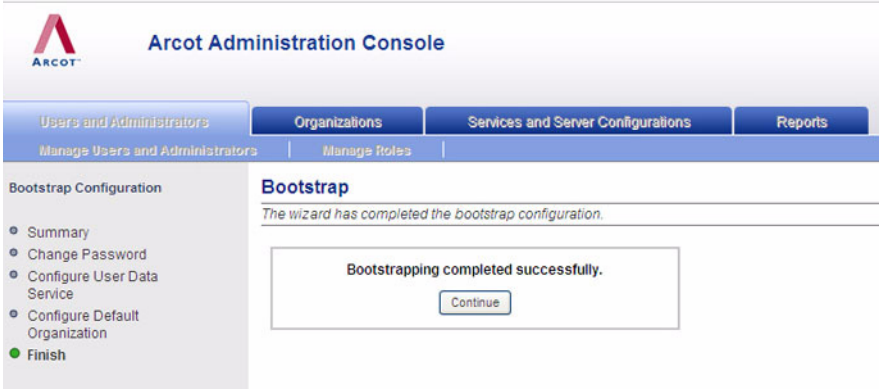
   - **Display Name:** The descriptive name of the organization. This name appears on all other Administration Console pages and reports.
   - **Authentication Mechanism:** The mechanism that is used to authenticate administrators belonging to the Default Organization. Administration Console supports 2 types of authentication methods for the administrators to log in:
     - **Basic User Password**

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

       If you select the **WebFort User Password** option here, then the credentials are issued and authenticated by the WebFort Server. Refer to *Arcot WebFort 6.0 Administration Guide* for more information on how to do this.

   The Administration Console initialization is completed, as indicated in the Finish screen (Figure 5-7).

Figure 5-7 Bootstrap Wizard: Finish Screen



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

Starting WebFort Server

Perform the following steps to start WebFort Server:

1. On the task bar, click the **Start** button.
2. Click **Settings**, and then point to **Control Panel**, **Administrative Tools**, and **Services.**
3. Select **Arcot WebFort Authentication Service**.
4. Click the **Start** button to start the service.

NOTE: If you want to stop the server, then click the **Stop** button.

Verifying the Installation

You can verify whether the WebFort Server and the Web applications have started successfully by:

- Using Log files
- Using arwfclient Tool
- Checking the Ports

Using Log files

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

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs`

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

   - `INSTANCE_VER.....: [6.0]`
   - `Arcot WebFort Authentication Service READY`

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

Using arwfclient Tool

The `arwfclient` tool enables you to check the version of WebFort you have installed. Refer to *Arcot WebFort 6.0 Administration Guide* for more information on this tool.

Perform the following steps to check the WebFort version:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\bin`

2. Execute **`arwfclient.exe`** with the following option:

   ```
   arwfclient ver
   ```

   The **`webfort-ver-<dd>-<mmm>-<yy>.txt`** file is created in the `<install_location>\Arcot Systems\logs folder.`

3. Open this file and check whether the version of library files is `6.0`.

Checking the Ports

Perform the following steps to verify if the WebFort Server is listening to different protocols on the default ports:

1. Navigate to the following location:

   `<install_location>\Arcot Systems\logs`

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

   ```
   PROTOCOLNAME : [Administration-WS]
   ```

```
PORTNO : 9745

PROTOCOLID : [Authentication-ASSP]
PORTNO : 9741

PROTOCOLID : [Authentication-Native]
PORTNO : 9742

PROTOCOLID : [Authentication-RADIUS]
PORTNO : 1812

PROTOCOLID : [Authentication-WS]
PORTNO : 9744
```

NOTE: Refer to **Appendix D, "Default Port Numbers and URLs"** for information on default ports and protocols.

Installing on Second System

After installing WebFort Server, Administration Console, and User Data Service 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. Locate the WebFort installer `Arcot-WebFort-6.0-Windows-Installer.exe` file.
2. Double-click the file `Arcot-WebFort-6.0-Windows-Installer.exe` to run the installer.
3. Follow the installer instructions from Step 3 on page 50 to reach the **Choose Install Set** screen.
4. Select the components you wish to install, typically you will be installing SDKs and the Sample Application. After you have selected the components, follow the steps from Step 9 on page 51 through Step 12 on page 54 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, Web services, and Sample Application:

- Deploying Sample Application
- Configuring Sample Application for WebFort Server

Deploying Sample Application

Sample Application can be used for testing WebFort or as a code sample for integrating ArcotID and other authentication methods into existing Web applications.

To deploy Sample Application:

1. Deploy the `webfort-6.0-sample-application.war` file from the following location:

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

2. Access the Sample Application in a Web browser window. The default URL for Sample Application is:

   `http://<host>:<port>/webfort-6.0-sample-application/`

Configuring Sample Application for WebFort Server

You must configure the Sample Application to communicate with WebFort Server, if they are installed on different systems. Perform the following steps to do so:

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

   `http://<host>:<port>/webfort-6.0-sample-application/`

   The WebFort 6.0 Sample Application page appears.

2. Click the **Setup** link.

3. Specify the values for the connection parameters listed in Table 5-4.

NOTE: The configurations made using these parameters are valid for the current session. You must set these values again if you restart the Sample Application or the application server.

Table 5-4 Connection Parameters

Field	Default Value	Description
Logger Configuration		
Log File Path	`./arcotwebfortsampleapp.log`	The relative path to the Sample Application log file. This path typically points to the main directory of your application server.
Server Configuration		
IP Address	localhost	The host name or the IP address where the WebFort Server is available.
Port	**Authentication Service:** `9742` **Issuance Service:** `9744`	The port on which the Authentication or the Issuance service is available.
Maximum Active Connections	`64`	The maximum number of database connections maintained by the Sample Application.

4. Click **Set Up** to save the connection.

To configure the Sample Application to communicate with an additional WebFort Server instance:

1. Click the **`[+]`** sign preceding **Additional Server Configuration**.
2. Specify the **IP Address** and **Port** connection parameters.
3. Click **Set Up** to configure the connection.

Chapter 6

Configuring Java SDKs and Web Services

This chapter describes the steps to configure the Java Software Development Kit (SDK) and Web services provided by WebFort.

Configuring Java SDKs

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

Configuring Authentication Java SDK

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

To configure Authentication SDK for using in a J2EE Application:

1. Copy the following JAR files from `<install_location>\Arcot Systems` to `<ApplicationHome>/WEB-INF/lib` directory
   - `sdk\java\lib\arcot\arcot-pool.jar`
   - `sdk\java\lib\arcot\arcot-webfort-authentication.jar`
   - `sdk\java\lib\arcot\arcot-webfort-common.jar`
   - `sdk\java\lib\external\bcprov-jdk14-139.jar`
   - `sdk\java\lib\external\commons-httpclient-3.1.jar`
   - `sdk\java\lib\external\commons-lang-2.0.jar`
   - `sdk\java\lib\external\commons-pool-1.4.jar`
   - `sdk\java\lib\external\log4j-1.2.14.jar`
2. Copy the `webfort.authentication.properties` configuration file containing the server connection parameters from `<install_location>\Arcot Systems\sdk\java\properties` to `<ApplicationHome>/WEB-INF/classes/properties`.

   NOTE: To know more about APIs and their initialization, refer to *Arcot WebFort 6.0 Java Developer's Guide* and the WebFort Javadocs at `<install_location>\Arcot Systems\docs\webfort\Arcot-WebFort-6.0-authentication-sdk-javadocs.zip`.

Configuring Web Services

If you are using Web services, then generate the client by using **`ArcotWebFortAuthSvc.wsdl`** file at `<install_location>\Arcot Systems\wsdls\webfort`.

Configuring Issuance Java SDK

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

To configure Issuance SDK for using in a J2EE Application:

1. Copy the following JAR files from `<install_location>\Arcot Systems` to `<ApplicationHome>/WEB-INF/lib` directory
   - `sdk\java\lib\arcot\arcot-pool.jar`
   - `sdk\java\lib\arcot\arcot-webfort-common.jar`
   - `sdk\java\lib\arcot\arcot-webfort-issuance.jar`
   - `sdk\java\lib\external\activation-1.1.jar`
   - `sdk\java\lib\external\axiom-api-1.2.7.jar`
   - `sdk\java\lib\external\axiom-impl-1.2.7.jar`
   - `sdk\java\lib\external\axis2-adb-1.4.jar`
   - `sdk\java\lib\external\axis2-java2wsdl-1.4.jar`
   - `sdk\java\lib\external\axis2-kernel-1.4.jar`
   - `sdk\java\lib\external\backport-util-concurrent-2.2.jar`
   - `sdk\java\lib\external\bcprov-jdk14-139.jar`
   - `sdk\java\lib\external\commons-codec-1.3.jar`
   - `sdk\java\lib\external\commons-collections-3.1.jar`
   - `sdk\java\lib\external\commons-httpclient-3.1.jar`
   - `sdk\java\lib\external\commons-lang-2.0.jar`
   - `sdk\java\lib\external\commons-logging-1.1.jar`
   - `sdk\java\lib\external\commons-pool-1.4.jar`
   - `sdk\java\lib\external\geronimo-spec-jms-1.1-rc4.jar`

- sdk\java\lib\external\log4j-1.2.14.jar
- sdk\java\lib\external\neethi-2.0.jar
- sdk\java\lib\external\stax-api-1.0.1.jar
- sdk\java\lib\external\wsdl4j-1.6.2.jar
- sdk\java\lib\external\wstx-asl-3.2.0.jar
- sdk\java\lib\external\XmlSchema-1.2.jar

2. Copy the webfort.issuance.properties configuration file containing the server connection parameters from <*install_location*>\Arcot Systems\sdk\java\properties to <*ApplicationHome*>/WEB-INF/classes/properties.

   NOTE: To know more about APIs and their initialization, refer to *Arcot WebFort 6.0 Java Developer's Guide* and the Issuance Javadocs at <*install_location*>\Arcot Systems\docs\webfort\Arcot-WebFort-6.0-issuance-sdk-javadocs.zip.

Configuring Web Services

If you are using Web services, then generate the client by using the **ArcotWebFortIssuanceSvc.wsdl** file at the location <*install_location*>\Arcot Systems\wsdls\webfort.

Enabling SSL Communication

WebFort supports Secure Socket Layer (SSL) between the WebFort Server and Java SDKs. The **Appendix F, "Configuring for SSL"** describes how to set the transport mode as SSL between the WebFort Server and its clients.

Chapter 7

Uninstalling WebFort

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

Uninstalling WebFort Schema

To uninstall WebFort schema from the database:

1. Based on the database type you are using, navigate to the folder:

For Oracle: `<install_location>\Arcot Systems\dbscripts\oracle`

For MS SQL: `<install_location>\Arcot Systems\dbscripts\mssql`

2. Run the scripts *in the following order*:
   a. `drop-webfort-6.0.sql`
   b. `drop-arcot-common-1.0.sql`

   This deletes all the database tables.

Uninstalling WebFort

Perform the following tasks to uninstall WebFort:

1. Stop WebFort Server.
2. Delete the DSN entry created during the WebFort installation by using the following steps:
   a. Go to Control Panel, and then open **Administrative Tools.**
   b. Open **Data Sources** (**ODBC**).
   c. Click the **Select System DSN** tab.
   d. Select the required DSN, and click **Remove**.
3. Ensure that INI files are not open in any editor.
4. Navigate to `<%SystemDrive%>\Program Files\Arcot Systems\Uninstall_Arcot WebFort directory.`
5. Double-click the `Uninstall Arcot WebFort.exe` file.

   The Uninstall Options screen appears.
6. Select **Complete Uninstall** to uninstall all the components of WebFort and go to Step 8. To uninstall the selected components select **Uninstall Specific Features** and click the **Next** button.

   The Choose Product Features screen appears.
7. This screen displays the WebFort components that are installed on the system. Select the components you wish to uninstall and click the **Next** button.

   The Uninstallation Complete screen appears at the end of successful uninstallation.
8. Select **Yes, restart my system** to restart the system after completing the uninstallation process.
9. Click **Done** to exit the installation wizard.

Post-Uninstallation Steps

The following are the post-uninstallation steps:

1. Delete the `<install_location>\Arcot Systems` folder.
2. Uninstall the following Web applications:
   - `arcotadmin` - Administration Console
   - `arcotuds` - User Data Service
   - `webfort-6.0-sample-application` - Sample Application

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

Verifying the Uninstallation

Perform the following steps to verify uninstallation of WebFort:

1. Go to **Control Panel**, and then open **Add or Remove Programs**.
2. Look for **Arcot WebFort** in **Currently installed programs** list.

   If the entry is not mentioned in the list, then the uninstallation is successful.

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:** Do not delete any of the files that are installed by WebFort.

WebFort Server Files

The following table lists the folder location of the files that are used by WebFort Server.

Table A-1 WebFort Server Files

Folder	File Description
<*install_location*>\	Contains **arcotkey** and **wfkey** files. These file are used by the installer to detect previously installed Arcot products. If you delete these 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.
<*install_location*>\Arcot Systems\bin	Contains the following executables that are required by administrators: • `arwfclient.exe` - Is used to shut down and refresh the WebFort Server. • `arwfserver.exe` - Is used to set the server management port and other server-related operations. • `dbutil.exe` - Is used for database-related operations.
<*install_location*>\Arcot Systems\conf	Contains the following configuration files: • **arcotcommon.ini** • `securestore.enc`
<*install_location*>\Arcot Systems\dbscripts\	Contains the SQL scripts to create the WebFort schema. See "Running Database Scripts," for information on the database scripts.
<*install_location*>\Arcot Systems\logs	Contains the installation and WebFort Server log file.
<*install_location*>\Arcot Systems\odbc32v60wf	Contains the branded DataDirect ODBC libraries for all the databases supported by WebFort.

Table A-1 WebFort Server Files

Folder	File Description
<*install_location*>\Arcot Systems\Uninstall_Arcot WebFort	Contains the executable required to uninstall WebFort.

Administration Console Files

The following table lists the folder location of the files that are used by Administration Console.

Table A-2 Administration Console Files

Folder	File Description
<*install_location*>\	Contains **arcotkey** and **wfkey** files. These file are used by the installer to detect previously installed Arcot products. If you delete these 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.
<*install_location*>\Arcot Systems\bin	Contains the following executable that is required by administrators: • `dbutil.exe` - This tool is used for database-related operations.
<*install_location*>\Arcot Systems\conf	Contains the following configuration files: • **arcotcommon.ini** • **adminserver.ini** • `securestore.enc`
<*install_location*>\Arcot Systems\dbscripts\	Contains the SQL scripts to create the Administration Console schema. See "Running Database Scripts," for information on the database scripts.
<*install_location*>\Arcot Systems\java\webapps	Contains the `arcotadmin.war` file required to deploy Administration Console.
<*install_location*>\Arcot Systems\java\ext	Contains the `arcot-crypto-util.jar` and `ArcotAccessKeyProvider.dll` file that is used to read the contents of `securestore.enc` file.
<*install_location*>\Arcot Systems\logs	Contains the Administration Console log file.

Table A-2 Administration Console Files

Folder	File Description
<*install_location*>\Arcot Systems\resourcepacks	Contains the following WebFort and Administration Console packages: • bundle_webfort.zip • bundler_adminconsole.zip
<*install_location*>\Arcot Systems\tools\bundlemanager	The folder contains the following files: • bundle-manager.jar • bundle_installer.xml

User Data Service Files

The following table lists the folder location of the files that are used by User Data Service.

Table A-3 User Data Service Files

Folder	File Description
<*install_location*>\	Contains **arcotkey** and **wfkey** files. These file are used by the installer to detect previously installed Arcot products. If you delete these 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.
<*install_location*>\Arcot Systems\bin	Contains the following executable that is required by administrators: • `dbutil.exe` - This tool is used for database-related operations.
<*install_location*>\Arcot Systems\conf	Contains the following configuration files: • **arcotcommon.ini** • **udsserver.ini** • `securestore.enc`
<*install_location*>\Arcot Systems\dbscripts\	Contains the SQL scripts to create the Administration Console schema. See "Running Database Scripts," for information on the database scripts.
<*install_location*>\Arcot Systems\java\webapps	Contains the `arcotuds.war` file required to deploy and User Data Service.
<*install_location*>\Arcot Systems\java\ext	Contains the `arcot-crypto-util.jar` and `ArcotAccessKeyProvider.dll` file that is used to read the contents of `securestore.enc` file.
<*install_location*>\Arcot Systems\logs	Contains the UDS log file.

Authentication Java SDK Files

The following table lists the folder location of the files that are used by Authentication Java SDK.

Table A-4 Authentication Java SDK Files

Folder	File Description
<*install_location*>\Arcot Systems\docs\webfort	Contains the Arcot-WebFort-6.0-authentication-sdk-javadocs.zip file, which contains the Javadocs for Authentication SDK.
<*install_location*>\Arcot Systems\samples\java	Contains the webfort-6.0-sample-application.war file to deploy Sample Application.
<*install_location*>\Arcot Systems\sdk\java\lib\arcot	Contains the following JAR files for WebFort Authentication Java SDK. • arcot-pool.jar • arcot-webfort-common.jar • arcot-webfort-authentication.jar
<*install_location*>\Arcot Systems\sdk\java\lib\external	Contains the third-party JAR files required by WebFort Authentication Java SDK. • bcprov-jdk14-139.jar • commons-httpclient-3.1.jar • commons-lang-2.0.jar • commons-pool-1.4.jar • log4j-1.2.14.jar
<*install_location*>\Arcot Systems\sdk\java\lib\properties	Contains the webfort.authentication.properties file.

Issuance Java SDK Files

The following table lists the folder location of the files that are used by Issuance Java SDK.

Table A-5 Issuance Java SDK Files

Folder	File Description
<*install_location*>\Arcot Systems\docs\webfort	Contains the Arcot-WebFort-6.0-issuance-sdk-javadocs.zip file, which contains the Javadocs for Issuance SDK.
<*install_location*>\Arcot Systems\samples\java	Contains the webfort-6.0-sample-application.war file to deploy Sample Application.
<*install_location*>\Arcot Systems\sdk\java\lib\arcot	Contains the following JAR files for Issuance Java SDK. • arcot-pool.jar • arcot-webfort-common.jar • arcot-webfort-issuance.jar

Table A-5 Issuance Java SDK Files

Folder	File Description
<*install_location*>\Arcot Systems\sdk\java\lib\external	Contains the third-party JAR files required by WebFort Issuance Java SDK. • activation-1.1.jar • axiom-api-1.2.7.jar • axiom-impl-1.2.7.jar • axis2-adb-1.4.jar • axis2-java2wsdl-1.4.jar • axis2-kernel-1.4.jar • backport-util-concurrent-2.2.jar • bcprov-jdk14-139.jar • commons-codec-1.3.jar • commons-collections-3.1.jar • commons-httpclient-3.1.jar • commons-lang-2.0.jar • commons-logging-1.1.jar • commons-pool-1.4.jar • geronimo-spec-jms-1.1-rc4.jar • log4j-1.2.14.jar • neethi-2.0.jar • stax-api-1.0.1.jar • wsdl4j-1.6.2.jar • wstx-asl-3.2.0.jar • XmlSchema-1.2.jar
<*install_location*>\Arcot Systems\sdk\java\lib\properties	Contains the webfort.issuance.properties file.

WSDL Files

The following table lists the folder location of the files that are used by Authentication and Issuance WSDLs.

Table A-6 WSDL Files

Folder	File Description
<*install_location*>\Arcot Systems\docs\webfort	Contains the following WSDL documents: • Arcot-WebFort-6.0-authentication-wsdldocs.zip • Arcot-WebFort-6.0-issuance-wsdldocs.zip

Plug-In SDK

The following table lists the folder location of the files that are used by plug-in SDK.

Table A-7 Plug-In SDK Files

Folder	File Description
<*install_location*>\Arcot Systems\bin	Contains the `arwfpluginsdk.dll` containing the plug-in libraries.

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 WebFort configuration files are available in the `<install_location>\Arcot Systems\Conf` location:

- **arcotcommon.ini**
- **adminserver.ini**
- **udsserver.ini**

The following properties files are available in the `<install_location>\Arcot Systems\sdk\java\properties\` location:

- **webfort.authentication.properties**
- **webfort.issuance.properties**

INI Files

arcotcommon.ini

The `arcotcommon.ini` file contains the parameters for database and instance settings for the WebFort Sever and other components (Administration Console and User Data Service) of WebFort. This section discusses these parameters of `arcotcommon.ini` file:

- **Parameters Used by WebFort Server**
- **Parameters Used by Administration Console and User Data Service**

Parameters Used by WebFort Server

The following table lists the database settings used by WebFort Server. Additional database configurations for the WebFort Server must be performed using the Instance Management screen of the Administration Console.

Table B-1 WebFort Server Parameters

Section	Parameter	Default	Description
`[arcot/db/dbconfig]`	`DbType`	No default	The type of the database applicable to all database connections. The supported values are: • oracle • mssqlserver
	`EnableBrandLicensing`	0	Whether a branded ODBC driver is in use. This can be used when you are using the branded ODBC drivers from DataDirect.
	`BrandLicenseFile`	No Default	The license file name when you use a branded ODBC driver.

Table B-1 WebFort Server Parameters

Section	Parameter	Default	Description
[arcot/db/primarydb] (*for primary database*)	Datasource.<*N*>	No Default	The name of the ODBC System Data Source Name (DSN) pointing to the primary database hosting the server data.
or [arcot/db/backupdb] (*for backup database*)	Username.<*N*>	No Default	The User Name used by the server to access the database.

Parameters Used by Administration Console and User Data Service

The following table lists the database setting parameters in the `arcotcommon.ini` file and provides descriptions of each.

Table B-2 Administration Console and User Data Service Parameters

Section	Parameter	Default	Description
`[arcot/db/dbconfig]`	`DbType`	No default	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` • For SQLServer - `com.microsoft.sqlserver.jdbc.SQLServerDriver`
	`MaxConnections`	32	The maximum number of connections that can be created between WebFort components and the database.
	`MinConnections`	4	The minimum number of connections to initially create between WebFort components and the database.

Table B-2 Administration Console and User Data Service Parameters

Section	Parameter	Default	Description
[arcot/db/dbconfig]	IncConnections	2	The number of connections that are created when a new connection is needed between WebFort components and the database.
	MaxIdleConnections	4	The maximum number of idle database connections that server can maintain.
	MaxWaitTimeForConnection	30000	Maximum amount of time (in milliseconds) the Server must wait (when there are no available connections) for a connection to become available, before timing out.
	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 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 the database messages are being logged. Set to 1 if you want to enable logging of database messages.
	EnableBrandLicensing	0	Whether a branded ODBC driver is in use. This can be used when you are using the branded ODBC drivers from DataDirect.
	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.

Table B-2 Administration Console and User Data Service Parameters

Section	Parameter	Default	Description
[arcot/db/dbconfig]	TransactionRetrySleepTime	10	The time difference between the transaction retries. This value is in millisecond.
[arcot/db/primarydb] (*for primary database*) or [arcot/db/backupdb] (*for backup database*)	Datasource.<*N*>		The name of the ODBC System Data Source Name (DSN) pointing to the primary database hosting the server data.
	AppServerConnectionPoolName.<*N*>		If the database connection pooling of the application server is used, then specify the JNDI name used to look up the connection pool object. A pool by this JNDI name should be created in the containing application server, and sufficient access right must be given to Arcot Web applications for it to use the connection pool. If the JNDI name is configured in Tomcat, then use a fully qualified JNDI name. For example, AppServerConnectionPoolName.1=java:comp/env/SampleDS For other application servers, specify only the JNDI name. For example, AppServerConnectionPoolName.1=SampleDS See **Appendix E, "Configuring Application Server"** for more information. If Application Server connection pool is *not* required, then leave this configuration empty.
	URL.<*N*>	No default	The name of the JDBC data source. • For Oracle - jdbc:oracle:thin:<*server*>:<*port*>:<*sid*> • For SQLServer - jdbc:sqlserver://<*server*>:<*port*>;databaseName=<*databasename*>;selectMethod=cursor
	Username.<*N*>	No default	The User Name used by the server to access the database.

Table B-2 Administration Console and User Data Service Parameters

Section	Parameter	Default	Description
[arcot/system]	InstanceId	1	A parameter that can be used to identify Administration Console or User Data Service instance. It is recommended that you provide unique values for every instance of the server. The instance ID is also displayed in the transaction reports. You must specify an integer value for this parameter.

adminserver.ini

The adminserver.ini file contains the parameters to set the Administration Console log information. The following table lists the log file information of Administration Console.

Table B-3 Log Parameters

Parameter	Description
• log4j.logger.com.arcot.admin • log4j.logger.com.arcot.database • log4j.logger.com.arcot.admin.framework • log4j.logger.com.arcot.adminconsole • log4j.logger.com.arcot.common.database	Specify the log level that must be used to write Administration Console logs. The supported log levels are: • FATAL • WARNING • INFO • DEBUG **NOTE:** Refer to *Arcot WebFort 6.0 Administration Guide* for more information on the log levels.
log4j.appender.debuglog.File	Specify the log file name and the location where the Administration Console logs must be written to. By default, the Administration Console log file name is arcotadmin.log and is created in the logs folder present in <*install_location*>\Arcot Systems\.
log4j.appender.debuglog.MaxFileSize	Specify the size of the log file. By default, it is 2 MB.

Table B-3 Log Parameters

Parameter	Description
`log4j.appender.debuglog.MaxBackupIndex`	Specify the number of backup files that can be created. When the number of backup files is equivalent to this number, the application starts to overwrite from the first log file.

udsserver.ini

The `udsserver.ini` file contains the parameters to set the User Data Service (UDS) log information. The following table lists the log file information of UDS.

Table B-4 Log Parameters

Parameter	Description
• `log4j.logger.com.arcot.uds` • `log4j.logger.com.arcot.common.database`	Specify the log level that must be used to write UDS logs. The supported log levels are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` **NOTE:** Refer to *Arcot WebFort 6.0 Administration Guide* for more information on the log levels.
`log4j.appender.debuglog.File`	Specify the log file name and the location where the UDS logs must be written to. By default, the UDS log file name is `arcotuds.log` and is created in the `logs` folder present in `<install_location>\Arcot Systems\`.
`log4j.appender.debuglog.MaxFileSize`	Specify the size of the log file. By default, it is 2 MB.
`log4j.appender.debuglog.MaxBackupIndex`	Specify the number of backup files that can be created. When the number of backup files is equivalent to this number, the application starts to overwrite from the first log file.

Properties Files

webfort.authentication.properties

The `webfort.authentication.properties` file provides the parameters for the Authentication Java SDK to read WebFort Server information. The following table lists the configuration parameters.

Table B-5 Parameters for Authentication Java SDK

Parameter	Default	Description
`authentication.host.1`	localhost	Hot name or the IP address of WebFort Server.
`authentication.port.1`	9742	Port number configured for the Authentication Native protocol.
`authentication.transport`	TCP	To enable the SSL communication between WebFort Authentication SDK and WebFort Server set this parameter to `SSL`. **NOTE:** If you change the transport mode to SSL, then you must restart WebFort Server.
`authentication.connectionTimeout`	10000	Maximum time in milliseconds before the WebFort Server is considered unreachable.
`authentication.readTimeout`	30000	The maximum time in milliseconds allowed for a response from WebFort Server.
`pool.maxActive`	32	Maximum number of connections allowed in the pool from the SDK to the WebFort Server.
`pool.maxIdle`	8	The maximum number of idle connections allowed in the pool from the SDK to the WebFort Server.
`pool.maxWaitTimeMillis`	-1	The maximum amount of time (in milliseconds) that a request will wait for the connection. Default -1 indicates that the thread will wait for infinite time.
`pool.minEvictableIdleTimeMillis`	30000	The minimum amount of time a connection might be idle in the pool before it is evicted by the idle connection evictor (if any).

Table B-5 Parameters for Authentication Java SDK

Parameter	Default	Description
pool.timeBetweenEvictionRunsMillis	300000	The amount of time in milliseconds to sleep before checking the pool to evict the idle connections.
authentication.serverCACertPEMPath	No Default	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.CACertPEMPath=<%*SystemDrive*%>/certs/webfort_ca.pem
authentication.clientCertKeyP12Path	No Default	Provide the path for the client certificate, which is in the p12 format.
authentication.clientCertKeyPassword	No Default	Enter the client key pair password to open the p12 file.

The webfort.authentication.properties file also contains the log file information for Authentication Java SDK. Set log4j.rootLogger and log4j.logger.com.arcot parameters to the required log level. Refer to *Arcot WebFort 6.0 Administration Guide* for more information on the log levels.

webfort.issuance.properties

The webfort.issuance.properties file provides the parameters for the Issuance Java SDK to read WebFort Server information. The following table lists the configuration parameters.

Table B-6 Parameters for Issuance Java SDK

Parameter	Default	Description
issuance.host.1	localhost	Hot name or the IP address of WebFort Server.
issuance.port.1	9744	Port number configured for the Transaction Web Services protocol.

Table B-6 Parameters for Issuance Java SDK

Parameter	Default	Description
issuance.transport	TCP	To enable the SSL communication between WebFort Issuance SDK and WebFort Server set this parameter to SSL. **NOTE:** If you change the transport mode to SSL, then you must restart WebFort Server.
issuance.connectionTimeout	10000	Maximum time in milliseconds before the WebFort Server is considered unreachable.
issuance.readTimeout	30000	The maximum time in milliseconds allowed for a response from WebFort Server.
pool.maxActive	32	Maximum number of connections allowed in the pool from the SDK to the WebFort Server.
pool.maxIdle	8	The maximum number of idle connections allowed in the pool from the SDK to the WebFort Server.
pool.maxWaitTimeMillis	-1	The maximum amount of time (in milliseconds) that a request will wait for the connection. Default -1 indicates that the thread will wait for infinite time.
pool.minEvictableIdleTimeMillis	30000	The minimum amount of time a connection might be idle in the pool before it is evicted by the idle connection evictor (if any).
pool.timeBetweenEvictionRunsMillis	300000	The amount of time in milliseconds to sleep before checking the pool to evict the idle connections.
issuance.serverCACertPEMPath	No Default	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.CACertPEMPath=<*%SystemDrive%*>/certs/webfort_ca.pem
issuance.clientCertKeyP12Path	No Default	Provide the path for the client certificate, which is in p12 format.
issuance.clientCertKeyPassword	No Default	Enter the client key pair password to open the p12 file.

The `webfort.issuance.properties` file also contains the log file information for Issuance Java SDK. Set `log4j.rootLogger` and `log4j.logger.com.arcot` parameters to the required log level. Refer to *Arcot WebFort 6.0 Administration Guide* for more information on the log levels.

Appendix C

Database Reference

WebFort Database contains a number of tables, some of which grow in size with increased usage of the product. Some tables grow in direct relation to the number of users, while others grow in direct relation to the usage of the product. This appendix provides the list of database tables that you can truncate to manage your disk space and improve the database performance.

> **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 database table replication. The following topics are covered in this appendix:

- Database Tables and Replication Advice
- Database Sizing Calculations
- Database Tuning Parameters

Database Tables and Replication Advice

This section lists and describes the database tables provided by WebFort and also provides the advice on how frequently the tables must be replicated between the primary and the backup databases. The following topics are covered in this section:

- Tables That Need Real-Time Synchronization
- Tables That Need Periodic Synchronization
- Tables That Do Not Need Synchronization

Tables That Need Real-Time Synchronization

The following table lists the database tables that need real-time synchronization between the primary and the backup databases. This category mainly includes the tables that contain user-related information and this data is required for authentication, therefore you must perform real-time synchronization of these tables.

Table C-1 Real-Time Synchronization Tables

Table	Description
ARADMINBASICAUTHUSER	Contains the basic authentication credentials of the administrators.
ARADMINSCOPE	Contains the information of the set of organizations over which an administrator has control.
ARADMINSCOPEALL	Contains the list of administrator who has control over all the organizations that are existing and those that will be created in future.
ARADMINUSER	Contains the information of an administrator.
ARADMINTXID	Contains the information required to generate transaction ID.
ARUDSORGANIZATION	Contains organization definitions, their attributes and repository connectivity details.
ARUDSUSER	Contains user details and attributes of the users belonging to the ARUSER organization. Also contains PAM, if any, for all types of users.
ARUDSAUTHSESSION	Contains authentication session details for currently active sessions. If this table is not replicated, then active authentication session can be lost.

Table C-1 Real-Time Synchronization Tables

Table	Description
ARWFARCOTID	Contains the ArcotID credentials for the users. It contains an individual entry for each user.
ARWFAUTHTOKENS	Contains the authentication tokens that are generated after a successful authentication. One entry is made in this table for every successful authentication irrespective of the type of token requested.
ARWFINSTANCES	Contains information about all the instances of WebFort Server that communicate with a specific database.
ARWFGENERICCRED	Contains the information about the miscellaneous credentials of the user. For example, the credentials supported by custom APIs.
ARWFOTP	Contains the One-Time Password (OTP) credentials for the users. It contains an individual entry for each user.
ARWFQNA	Contains the Question and Answer (QnA) credentials for the users. It contains an individual entry for each user.
ARWFPASSWORD	Contains the user name-password credentials for the users. It contains an individual entry for each user.
ARWFVERIFIEDCHALLENGES	Contains information about the challenges for which the ArcotID signature is successfully verified. An entry is made for successful ArcotID authentication, provided `No Replay` for challenge is turned on. It is turned off by default.

Tables That Need Periodic Synchronization

The following table lists the database tables that need periodic synchronization between the primary and the backup databases. These database tables are synchronized when there is any change in the configurations.

Table C-2 Periodic Synchronization Tables

Table	Description
ARADMINCONFIG	Contains the Administration Console configurations.
ARADMINCUSTOMROLE	Contains the configurations for custom defined role.
ARADMINMAP	Contains the information of the WebFort Server instance, which is entered as a key-value pair.

Table C-2 Periodic Synchronization Tables

ARADMINPAFCONFIG	Contains administrator authentication configuration for an organization.
ARADMINPWDPOLICY	Contains the administrator password policies for all the organizations.
ARADMINTURNEDOFFPRIVILEGE	Contains the information about the privileges that are not available for the custom role.
ARADMINCACHEREFRESH	Contains cache refresh information that decides whether the Administration Console need to refresh the cache.
ARADMINAUDITTRAIL	Contains administrator activity audit.
ARUDSAUDITLOG	Contains the audit log information for the User Data Source (UDS) operations and their return status.
ARUDSCONFIG	Contains the UDS configuration parameters and their values.
ARUDSREPOSITORYTYPES	Contains the definitions of the repository supported by UDS. This table is expected to change only when new plug-ins are added to the system.
ARUDSUSERATTRIBUTE	Contains the user attribute definitions. This table is expected to change rarely, only when new user attributes are added by individual products.
ARWFADMINAUDITLOG	Contains the audit log information for the WebFort administration activities.
ARWFARCOTIDHISTORY	Contains all the ArcotIDs that are in *re-issue* state.
ARWFAUTHAUDITLOG	Contains the audit log information for the authentication activities.
ARWFCONFIG	Contains the WebFort configuration information. The information in this table contains version information and therefore has multiple entries per configuration.
ARWFCUSTOMCONFIG	Contains the WebFort plug-in configuration information. The information in this table contains version information and therefore has multiple entries per configuration.
ARWFGENERICCREDHISTORY	Contains all the miscellaneous (for example, custom API supported) credentials that are in *re-issue* state.
ARWFISSUANCEAUDITLOG	Contains the audit log information for the credential issuance activities.
ARWFMODULEREGISTRY	Contains information about the internal modules of the WebFort Server and about the plug-ins.

Table C-2 Periodic Synchronization Tables

ARWFORGACTIVECONFIG	Contains configuration mapping of the currently active organization. The information in this table contains version information and therefore has multiple entries per configuration.
ARWFORGCONFIG	Contains configuration mapping per organization. The information in this table contains version information and therefore has multiple entries per configuration.
ARWFOTPHISTORY	Contains all the one-time password credentials that are in *re-issue* state.
ARWFPASSWORDHISTORY	Contains all the user-name password credentials that are in *re-issue* state.
ARWFPROTOCOLCONFIGURATION	Contains configuration of each listener port of the WebFort Server.
ARWFQNAHISTORY	Contains all the question and answer credentials that are in *re-issue* state.
ARWFSEQUENCE	Contains information about sequences used for version configurations.
ARWFSSLTRUSTSTORE	Contains the SSL root certificates that are trusted by the WebFort Server.
ARWFSVRMGMTAUDITLOG	Contains the audit log information for the server management activities.

Tables That Do Not Need Synchronization

The following table lists the database tables that do not need any synchronization between the primary and the backup databases.

Table C-3 Tables that do not need Synchronization

Table	Description
ARCMNDBERRORCODES	Contains vendor-specific database error codes and SQL state values that signifies whether the database is down or non-responsive. This information is used to decide if database should be failed over, if a backup is configured.
ARADMINMANAGEROLE	Contains the list of roles that a role can manage.
ARADMINPREDEFINEROLE	Contains the role information for all supported administrators.

Table C-3 Tables that do not need Synchronization

Table	Description
ARADMINSUPPORTEDAUTHMECH	Contains the information about all supported authentication mechanisms.
ARADMINUITAB	Contains the information about Administration Console tabs.
ARADMINUITASK	Contains the information about the tasks that are performed using Administration Console.
ARADMINUITASKATTRIBUTES	Contains the details of the tasks that are displayed, when the first-level and the second-level tabs in the Administration Console are clicked. These tasks are referred to as landing pages.
ARADMINUITASKCONTAINER	Contains the information related to the task container. The task container can either be a second-level tab ID or the task group in the Administration Console.
ARADMINWIZARDTASK	Contains the information about the tasks that are performed using the Administration Console bootstrap wizard.
ARRFREPORTTABLES	Contains the metadata of other tables.
ARADMINMAPDATATYPE	Contains the list of data types that are supported in ARADMINMAP.
ARWFDBERRORCODES	Contains the database error codes that indicate the communication failure.
ARWFDBQUERIES	Contains the list of database queries used by WebFort Server.
ARWFDISPLAYNAMES	Contains names and values for different keys used in WebFort.
ARWFLOCALE	Contains the list of locales supported by WebFort.
ARWFMESSAGES	Contains the messages that are posted by the WebFort Server.

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

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

Considering the figures assumed in section, "Value Assumptions," 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 Tuning Parameters

The following table lists the common parameters that you can use to tune the connection between WebFort Server and the database. These configurations are made using the Instance Management screen of the Administration Console.

Table C-4 Connection Parameters Between WebFort Server and Database

Field	Description
Minimum Connections	The minimum number of connections to initially create between the WebFort Server and the database.
Maximum Connections	The maximum number of connections that can be created between the WebFort Server and the database. **NOTE:** You must set this value depending on the maximum connections that the database supports, because this overrides the `MaxConnections` parameter. See your database vendor documentation for more information.
Increment Connections by	The number of connections that will be added to the existing connections, when the need arises. The total number of connections cannot exceed the maximum number of connections.
Monitor Thread Sleep Time (in Seconds)	The amount of time the monitoring thread sleeps between heartbeat checks on all the databases.
Query Timeout	The amount of time for which the query posted by WebFort Server is valid. If the query is not served in this duration, then it will be closed.
Connection Retry Sleep Time (in Seconds)	The amount of time to delay between attempts to connect to the database.
Log Query Details	Enables you to log all the database queries.
Auto-Revert to Primary	Enables the server to switch from the backup to primary database when the primary database becomes functional.

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

WebFort supports four protocols that are configured at different ports. The following table lists the default port numbers used by WebFort.

Table D-1 WebFort Protocols

Protocol	Default Port Number	Default Status	Description
Server Management Web Services	9743	Enabled	This protocol is used for managing WebFort server. Administration Console and `arwf-client` clients communicate using this port for server management activities.
Transaction Web Services	9744	Enabled	This protocol is used by the Authentication and the Issuance Web services client to connect to WebFort Server.
Authentication Native	9742	Enabled	This is a proprietary, binary protocol used by WebFort for the purpose of authentication. This port is used by Authentication SDK.
Administration Web Services	9745	Enabled	This protocol is used to create and manage configurations, such as profiles, policies, SAML, and ASSP configurations.
RADIUS	1812	Disabled	This is used to support the Remote Authentication Dial In User Service (RADIUS) protocol. When configured to support RADIUS protocol, WebFort server acts as a RADIUS server.
ASSP	9741	Disabled	This protocol is used with Adobe® Reader and Adobe® Acrobat® to authenticate user for server-side digital signing of the PDF documents.

If some other service is already running on the default port, then you must set a new port for the protocols. To set new port number for Server Management Web Services protocol, use `webfortserver` tool, see Chapter 5, "Tools for System Administrators" in *Arcot WebFort 6.0 Administration Guide*. To set new port number for other protocols, use Protocol Configuration screen in the Administration Console, see Chapter 3, "Managing WebFort Server Instances" in *Arcot WebFort 6.0 Administration Guide*.

URLs for WebFort Components

Use the URLs listed in the following table to access WebFort components after installation.

Table D-2 Default Port Numbers

Component or Service	URL
Administration Console URL for Master Administrator	http://<*Apphost*>:<*port*>/arcotadmin/masteradminlogin.htm
Administration Console URL for other administrators	http://<*Apphost*>:<*port*>/arcotadmin/adminlogin.htm
Sample Application	http://<*Apphost*>:<*port*>/webfort-6.0-sample-application/

Appendix E

Configuring Application Server

This appendix outlines the steps that you must perform to set up the database connection pooling on the application server, where the WebFort components will be deployed. It covers the configuration steps for the following application servers:

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Apache Tomcat

This section provides the steps to enable Apache Tomcat for JNDI-based database operations.

Perform the following steps to create a JNDI connection in Apache Tomcat:

1. Install the Apache Tomcat application server and test the installation using the following URL:

   `http://localhost:8080/`

2. Open the **`server.xml`** file present in the `<TOMCAT-HOME>/conf` directory.

3. Collect the following information required to define a data source:

   - **JNDI Name**

     The JNDI name used by the arcot components. This name must match with the **AppServerConnectionPoolName`.<N>`** in `arcotcommon.ini` (without the `java:comp/env/` prefix).

   - **User ID**

     The database user ID.

   - **Password**

     The database password.

   - **JDBC Driver Class**

     The JDBC driver class name. For example, `oracle.jdbc.driver.OracleDriver`.

   - **JDBC URL**

     The JDBC URL for the database server. For example, if you are using Oracle driver, then URL would be: `jdbc:oracle:thin:<server>:<port>:<sid>`.

4. Add the following entry to define the datasource within the `<GlobalNamingResources>` tag:

```
<Resource name="SampleDS"
         auth="Container"
         type="javax.sql.DataSource"
        factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceF
        actory"
```

```
username="<userid>"
password="<password>"
driverClassName="<JDBC driver class>"
url="<jdbc-url>"
maxWait="30000"
maxActive="32"
maxIdle="8"
initialSize="4"
timeBetweenEvictionRunsMillis="300000"
minEvictableIdleTimeMillis="30000"/>
```

5. Open the **`context.xml`** file present in the <*TOMCAT-HOME*>/conf directory.
6. Add the following entry to define the datasource within the <Context> tag:

   ```
   <ResourceLink global="SampleDS" name="SampleDS"
   type="javax.sql.DataSource"/>
   ```

7. Copy the following database connection pooling (DBCP) dependencies to <*TOMCAT-HOME*>/common/lib directory.
   - commons-dbcp-1.2.2.jar
   - ojdbc14-10.2.0.1.0.jar (for Oracle database)
   - sqljdbc.jar (Microsoft JDBC driver for MS SQL Server 2005 - version 1.2.2828)

IBM WebSphere

This section provides the steps to enable IBM WebSphere for JNDI-based database operations:

Perform the following steps to configure IBM WebSphere for deploying Java-dependant components of the Arcot Adapter:

1. Log in to WebSphere Administration Console.
2. Select **Resources** and expand the **JDBC** node.
3. Select **JDBC Providers** and click **New** to create an appropriate JDBC provider depending on the database you are using.

   NOTE: Refer to `http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.iseries.doc/info/iseries/ae/tdat_ccrtprov.html`

4. Enter the database `CLASSPATH` information by following the on-screen instructions.
5. Click **Next** and verify the Summary page. Click **Finish** to complete the JDBC provider configuration.
6. Click **Save** to save the changes made.
7. Go to **Resources**, and then click **JDBC**.
8. Under **JDBC**, open **Data Sources** and click **New** to create a new data source. Perform the following steps to create a data source:
   a. Specify the data source name.
   b. Specify the JNDI Name. This name must match with the **AppServerConnectionPoolName.<N>** in `arcotcommon.ini`.
   c. Click **Next** and select the JDBC provider created in Step 3.
   d. Click **Next** and specify the JDBC URL.
   e. Select the data source and click **Next** and then **Finish**.
   f. Click **Next** to view the Summary screen and then click **Finish**.
9. Click **Save** to save the changes made.
10. Select the data source created in the preceding step and click **Related Items** section.

11. Select **New** to create a new credential.
12. Enter login credentials that are used to connect to the database and save the credential.
13. Click **Apply** and then **Save** to save the changes made.
14. Select **Data Sources** and select the data source that you created in Step 7.
15. Under **Component-managed authentication alias**, select the JAAS credential that you created in Step 12 and click **Save**.
16. Select **Data Sources** and select the check box for the data source you created in Step 7.
17. Click **Test connection** to verify that you have specified the connection correctly.

    NOTE: This test only checks the connection to the database server, not necessarily the correct definition of the data source.

BEA WebLogic

This section provides the steps to enable BEA WebLogic for JNDI-based database operations.

Perform the following steps to create a data source in BEA WebLogic:

1. Log in to WebLogic Administration Console.
2. Click the **Lock & Edit** button, if it is not done.
3. Go to **Resources**, and then click **JDBC**.
4. Under **JDBC**, open **Data Sources** and click **New** to create a new data source. Perform the following steps to create a data source.
5. Set the following JNDI and the database information:
    a. Set **Name** = ArcotDB.
    b. Set **JNDI Name** = ArcotDB.
    c. Choose a suitable **Database Type**, for example Oracle.
    d. Select a suitable **Database Driver**, for example Oracle Thin Driver.
6. Click **Next**, retain the default values and click **Next** again.
7. In the Connection Properties page, set the database details. The values mentioned here are for Oracle database:
    - **Database** = SID or service name of the DB server
    - **Hostname** = the DB server's IP address or host name
    - **Port** = 1521 or any other port the DB server is running
    - **Database User Name**
    - **Database Password / Confirm Password**
8. Click **Test Configuration** to verify that you have specified the correct database parameters.
9. Click **Next** and set the data source target to the preferred WebLogic server instance.
10. Click **Finish** to return to the data source list page.
11. Click **Activate** to enable the data source settings.

Appendix F

Configuring for SSL

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 SSL (Secure Socket Layer) transport mode.

The following steps list how to set up SSL between different components:

> **NOTE:** You *must* follow this order to set up SSL successfully. After completing every step, test whether connection has been set successfully.

1. Enable UDS for SSL
2. Between Administration Console and User Data Service
3. Between WebFort Server and User Data Service
4. Between Administration Console and WebFort Server
5. Between Authentication SDK and WebFort Server
6. Between Issuance SDK and WebFort Server

Enable UDS for SSL

The application server where User Data Service (UDS) is deployed must be enabled for SSL. Refer to your application server vendor documentation for more information.

Between Administration Console and User Data Service

If Administration Console and UDS are deployed on different application servers, then the application servers must be enabled for SSL. Refer to your application server vendor documentation for more information on how to set SSL.

Between WebFort Server and User Data Service

To set up SSL between WebFort Server and User Data Service (UDS), you must upload the certificates required for SSL by using the User Data Service Configuration page in the Bootstrap Wizard flow. See "Bootstrapping the System" for more information.

Between Administration Console and WebFort Server

To configure SSL-based communication between WebFort Server and Administration Console, you must configure the Server Management protocol to SSL mode:

1. Open Administration Console in a Web browser.
2. Log in to Administration Console using a Global Administrator account.
3. Under **WebFort Configurations** from the left-hand menu, select **Protocol Setup.**

   The WebFort Protocol Setup page appears.
4. Activate the **Services & Server Configurations** tab in the main menu.
5. Activate the **WebFort** tab in the submenu.
6. Under **System Configurations**, click the **Protocol Configuration** link to display the corresponding page.

   The Protocol Configuration page appears.
7. Select the **Server Instance** for which you want to configure the protocols.
8. In the **List of Protocols** section, select the **Server Management** protocol.

   The page to configure the protocol appears.
9. This page contains the fields listed in the following table.

Table F-1 Configuring Protocol

Field	Description
Protocol Status	Indicates whether the protocol is **Enabled** or **Disabled**.
Change the Protocol Status	Select this check box to change the status of the protocol, and then select the new status from the drop-down list. **NOTE:** The Server Management protocol cannot be disabled. Therefore the option to disable this protocol is not available.
Port	Enter the port number where the protocol service is available.
Minimum Threads	Enter the minimum number of threads to be maintained between the WebFort Server and the client.

Table F-1 Configuring Protocol

Field	Description
Maximum Threads	Enter the maximum number of threads that can exist between the WebFort Server and the client.
Transport	Specify the mode for data transfer. The following are the supported values: • **TCP** - Transmission Control Protocol (TCP) mode is supported by all WebFort network protocols other than WebFort RADIUS protocol. • **SSL** - SSL uses the PKI to encrypt and decrypt data under transmission.
Server Certificate Chain	Specify the server certificate chain that is used by the SSL transport security mode. Upload the Certificate Chain using the respective **Browse** button in the corresponding field.
Server Private Key	Specify the server private key that is used by the SSL transport security mode. Upload the Certificate Chain using the respective **Browse** button in the corresponding field.
Select Client Store	Select the trust store, which contains the root certificate of the trusted Certificate Authority (CA).

10. Click the **Save** button, after the configurations are completed.
11. Restart WebFort Server.
12. Restart Administration Console.

Between Authentication SDK and WebFort Server

To set up SSL between WebFort Server and Authentication Java SDK, you must configure the `webfort.authentication.properties` file at:

`<install_location>\Arcot Systems\sdk\java\properties`

See "webfort.authentication.properties" for more information on the configuration parameters.

Between Issuance SDK and WebFort Server

To set up SSL between WebFort Server and Issuance Java SDK, you must configure the `webfort.issuance.properties` file at:

`<install_location>\Arcot Systems\sdk\java\properties\`

See "webfort.issuance.properties" for more information on the configuration parameters.

Appendix G

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

Microsoft SQL Server 2005 JDBC Driver

Apache

- `log4j 1.2.9`
- `Axis2 1.4`
- `DBCP 1.2.2`
- `oro-2.0.7.jar`
- `velocity-1.5.jar`
- `standard-1.1.2.jar`
- `iBATIS 2.3.4.726`
- `geronimo-jms_1.1_spec-1.1.jar`
- `commons-beanutils-1.7.0.jar`

- commons-codec-1.3.jar
- commons-collections-3.1.jar
- commons-dbcp-1.2.2.jar
- commons-digester-1.7.jar
- commons-fileupload-1.1.1.jar
- commons-httpclient-3.1.jar
- commons-io-1.2.jar
- commons-lang-2.4.jar
- commons-logging-1.1.jar
- commons-pool-1.4.jar
- commons-validator-1.3.1.jar
- struts-1.2.8.jar

Spring Framework

- spring-2.5.2.jar
- spring-aop-2.5.2.jar
- spring-beans-2.5.2.jar
- spring-binding-1.0.5.jar
- spring-context-2.5.2.jar
- spring-context-support-2.5.2.jar
- spring-core-2.5.2.jar
- spring-dao-2.0.8.jar
- spring-ibatis-2.0.8.jar
- spring-jdbc-2.5.2.jar
- spring-jms-2.5.2.jar
- spring-orm-2.5.2.jar
- spring-test-2.5.2.jar
- spring-tx-2.5.2.jar
- spring-web-2.5.2.jar
- spring-webflow-1.0.5.jar

- `spring-webmvc-2.5.2.jar`
- `spring-webmvc-portlet-2.5.2.jar`
- `spring-webmvc-struts-2.5.2.jar`
- `springmodules-validation-0.4.jar`

Bouncy Castle 1.3.9

Sun Microsystems

- Java Mail
  - `mail-1.4.jar`
- JSTL
  - `jstl 1.0.3.jar`
- LDAP library
  - `ldap-1.2.4.jar`
- JDBC
  - `jdbc-1.2.2828.jar`
- Java Servlet
  - `servlet-api-2.3.jar`

cglib-2.1_3.jar

Licensed under Apache Software Foundation.

asm-1.5.3.jar

ognl-2.6.9.jar

aopalliance-1.0.jar

Licensed under AOP Alliance.

Appendix H

Glossary

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 hash function	A cryptographic hash function is a hash function with additional security properties, used in security-related applications such as authentication.
User Administrator	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.
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 situation.
Forgot Your Password (FYP)	If the user forgets their 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.
Failed attempts	The number of times the user failed to authenticate using a particular credential.

PKCS	PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA. See "public-key cryptography," for more details.
PKCS#7	It is used to sign and encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message).
private key	One 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 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.
Secure Hash Algorithm (SHA)	Secure Hash Algorithm (SHA) family is a set of cryptographic hash functions.
Secure Socket Layer (SSL)	SSL is a protocol intended to secure and authenticate communications across public networks by using data encryption.
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

T

U

V

W