Arcot Adapter™ for CA SiteMinder®
Installation and Configuration Guide
(UNIX Platforms)
Version 2.2

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot Adapter for CA SiteMinder Installation and Configuration Guide
Version 2.2
November 2010
Part Number: AA-0022-0IGU-01

Trademarks

Patents

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

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

Third Party Software

All the third-party software used by Arcot Adapter and related components are listed in Appendix C, “Third-Party Software Licenses”.

Contents

Preface

This guide describes the process to install and configure Arcot Adapter 2.2 with CA SiteMinder® Web Access Manager on Solaris (SPARC) and Red Hat Enterprise Linux platforms. This guide includes information on:

- High-level architecture of the integrated solution
- Components of Arcot Adapter
- Requirements for installing Arcot Adapter
- Installation and post-installation tasks
- Configuration of *Forms Credential Collector* (FCC) pages
- Arcot Adapter uninstallation process
- Support for Backing Authentication

Intended Audience

This guide is intended for system integrators who are responsible for configuring CA SiteMinder® Web Access Manager with Arcot WebFort and Arcot RiskFort to seamlessly work with each other. This guide requires that the reader must be familiar with Arcot WebFort, Arcot RiskFort, and CA SiteMinder® Web Access Manager authentication configurations, particularly custom authentication schemes and FCC pages.

Note: This guide assumes that CA SiteMinder® Web Access Manager, Arcot WebFort, and Arcot RiskFort have been installed and are independently operational, before you follow the procedures in this guide.

Information Included in this Guide

This guide is organized as follows:

- Chapter 1, “Arcot Adapter for CA SiteMinder® WAM Overview”, describes the high-level integration architecture of Arcot Adapter and describes the other Arcot products that Adapter interacts with.
- Chapter 2, “Preparing for Installation”, lists the prerequisite software and configurations required to install Arcot Adapter.
- Chapter 3, “Installing Arcot Adapter”, describes the steps to install the Arcot Adapter in normal and silent modes.
- Chapter 4, “Deploying and Configuring State Manager”, describes the steps to deploy and configure the State Manager.
- Chapter 5, “Deploying and Configuring Authentication Flow Manager”, describes the steps to deploy and configure the Authentication Flow Manager.
- Chapter 6, “Configuring Authentication Shim and FCC Pages”, describes the steps to configure the FCC pages and Arcot Authentication Shim.
- Chapter 7, “Configuring CA SiteMinder Policy Server”, describes the steps to configure CA SiteMinder® Web Access Manager to use the Adapter.
- Chapter 8, “Uninstalling Arcot Adapter Components”, lists the steps to uninstall the Arcot Adapter components and the database that is used by Arcot Adapter.
- Appendix A, “Configuring Backing Authentication Scheme”, describes the steps to configure support for external or third-party authentication schemes or mechanisms.
- Appendix B, “New File and Property Names”, lists the file names and properties that have been renamed in the current release of Arcot Adapter.
- Appendix C, “Third-Party Software Licenses”, lists the third-party software that are used with Adapter.
- Appendix D, “Glossary”, describes the terms that are used in this guide.

Related Publications

Other related Arcot publications are as follows:

Arcot WebFort 6.2 Installation and Deployment Guide	This guide describes the procedure for installing and deploying WebFort on supported platforms.
Arcot WebFort 6.2 Administration Guide	This guide provides information to administer and configure WebFort.
Arcot RiskFort 2.2.6 Installation and Deployment Guide	This guide describes the procedure for installing and deploying RiskFort on supported platforms.
Arcot RiskFort 2.2.6 Administration Guide	This guide provides information to administer and configure RiskFort.

Conventions Used in This Book

The conventions and formats used in this manual are described in the following paragraphs:

Typographical Conventions

This manual uses the following typographical conventions:

Italic	Emphasis, Guide names
Bold	User input, GUI screen text
`Fixed`	File and directory names, extensions, Command Prompt, CLI text, code in running text
`Fixed Bold`	Target file or directory name in the path
`Fixed`	Command Prompt, CLI text, code
`Fixed-Italic`	File or directory name that might be different from user to user
Link	Links within the guide, URL links

Formats

This manual uses the following formats to highlight special messages:

	**Note:** Highlights information of importance or special interest.
	**Tip:** Highlights a procedure that will save time or resources.
	**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.
	**Important:** Information to know before performing an operation.
	**Caution:** Makes the user attentive of the possible danger.
	**Book:** Provides reference to other guides.

Contacting Support

If you need help, contact Arcot Support as follows:

Email	*support@arcot.com*
Web site	*http://www.arcot.com/support/index.html*

Chapter 1
Arcot Adapter for CA SiteMinder® WAM Overview

CA Web Access Manager (also known as the *CA SiteMinder WAM*) provides centralized security management capability that enables customers, partners, and end users to securely access the Web to deliver applications and data. By integrating CA SiteMinder WAM with Arcot WebFort and RiskFort, you can additionally protect your resources with the multifactor and risk-based adaptive authentication that these Arcot products offer.

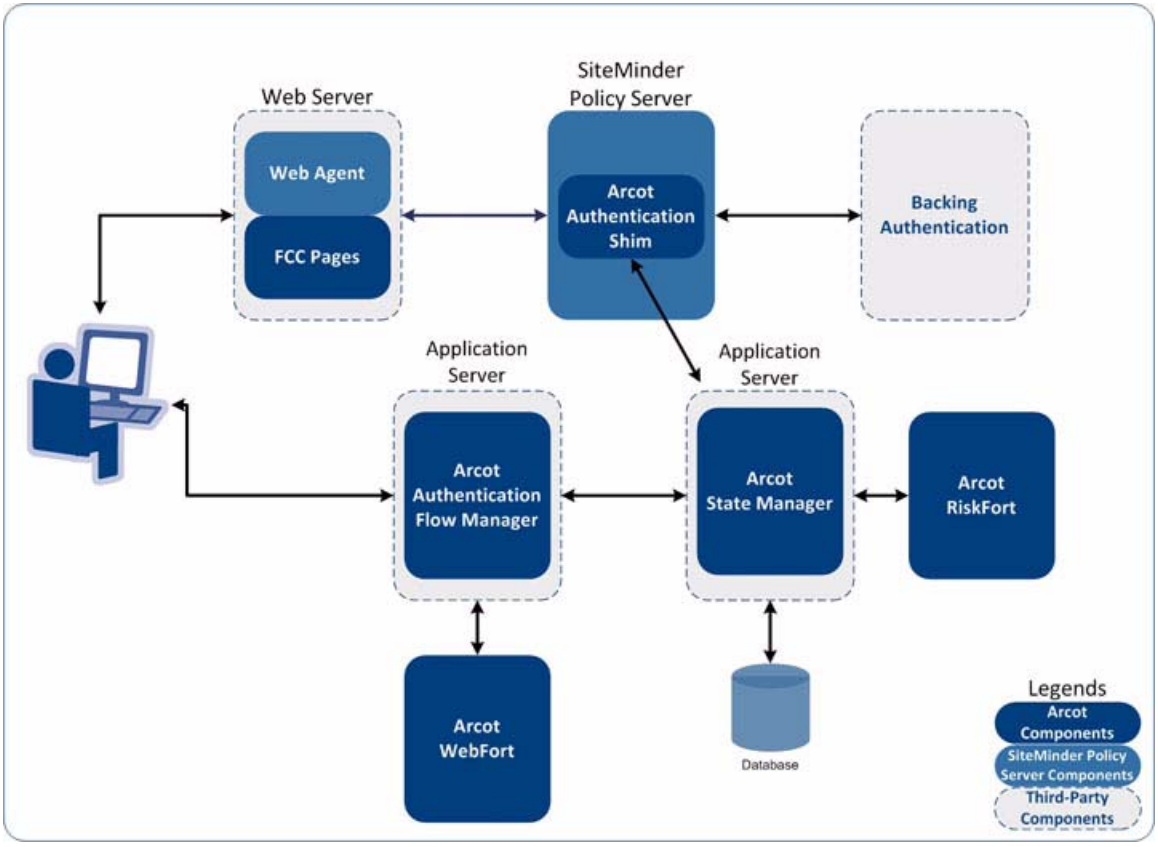
This chapter introduces you to the Arcot Adapter architecture, various components of the integrated solution, and the main features introduced in the current release of Arcot Adapter.

This chapter covers the following topics:

Adapter Architecture

The following figure illustrates how Arcot Adapter and its components integrate with the components of SiteMinder Policy Server.

Figure 1-1 Adapter Architecture Diagram



Note: In case you plan to use a single database for Arcot products and other applications, then Arcot strongly recommends that you use a separate schema for Arcot products.

As illustrated in the preceding figure, Arcot Adapter includes the following components:

- Arcot Authentication Flow Manager
- Arcot State Manager
- Arcot Authentication Shim
- Form Credential Collector (FCC) Pages

In addition, Adapter also uses other Arcot products which are explained in the section "Other Arcot Products Used With Adapter".

Arcot Authentication Flow Manager

The *Authentication Flow Manager* (AFM), which was earlier known as the *Arcot Customization Engine (ACE)*, serves as an interface between the user and other components of Arcot Adapter. It also performs the function of a state machine that guides the end user through the following *preconfigured authentication flows*:

- **ArcotID Authentication**: this includes ArcotID authentication using Arcot WebFort.
- **ArcotID and Risk Evaluation**: this authentication flow is a combination of ArcotID and Risk evaluation (performed by Arcot RiskFort) flows.
- **Primary Authentication and Risk Evaluation**: this authentication flow combines the primary authentication scheme, which is configured in SiteMinder, and the Risk evaluation flow. The risk evaluation can be configured to either precede or succeed the primary authentication, thus, offering two different authentication flows.

Typically, these authentication flows are rendered as the JavaServer Pages (JSPs). These JSPs collect the users' information required for authentication.

AFM also maintains the state data of the user's authentication flow, conducts WebFort authentication, and reads or writes information (specifically, RiskFort Device IDs) required by RiskFort.

Note: Not all user activities require user input. For example, risk assessment can be done without any user input.

In addition to the four sample authentication flows that AFM is shipped with, it also provides you the capability to customize and configure multiple authentication flows at any time.

Arcot State Manager

The *State Manager* (formerly known as the *Token Server*) is responsible for creating, maintaining, and tracking the tokens that are used to associate users' authentication and risk status across multiple Arcot and CA SiteMinder WAM components. The tokens, which contains the information of the user and the session state, enables other Arcot components to remain stateless.

This release of Arcot Adapter supports database failover for the State Manager. If the primary database server goes down or becomes unavailable, the State Manager can switch over to the secondary database server. The secondary database server is configured to run in a standby mode and it maintains an up-to-date replica of the primary server's data. This makes users' session information available all the time. To enable the failover support, a new set of parameters have been introduced in the State Manager properties file. For details on the parameters that you need to configure to enable the database failover, see "Database Connectivity Parameters" in Chapter 4.

The State Manager also acts as a proxy to the RiskFort by providing risk evaluation services to other Adapter components. It receives the risk evaluation input parameters from the calling application and passes it to RiskFort. After the risk evaluation is complete, the State Manager inserts the result of the risk evaluation into the token for further examination or for processing by other components.

Note: Based on the implemented workflow, risk evaluation can be performed *before* or *after* the user authentication. If the risk evaluation takes place after user authentication, the result of the authentication is persisted in the token and then the risk evaluation is performed.

The State Manager also provides a token and validation mechanism to securely communicate the authentication result, risk result, and the subsequent action to be performed by the Authentication Shim.

Arcot Authentication Shim

The *Arcot Authentication Shim*, which integrates with CA SiteMinder WAM, acts as an interface between the WAM and the Adapter components (State Manager and AFM), and other Arcot products (WebFort and RiskFort).

The Authentication Shim is an instance of a shared library and resides in the SiteMinder Policy Server instance. It supports the CA SiteMinder WAM Authentication API Provider interface.

Form Credential Collector (FCC) Pages

FCC pages are static HTML pages used by Arcot Authentication Shim to collect user inputs during basic or primary authentication and to display error messages, if any. These pages are deployed on the same Web Server where the SiteMinder Policy Server Web Agents reside.

Other Arcot Products Used With Adapter

This section provides a brief introduction to the following Arcot products that are used with Arcot Adapter:

- Arcot WebFort
- Arcot RiskFort

Arcot WebFort

Arcot WebFort protects users from identity theft and fraud by providing strong, two-factor authentication, without changing their familiar user name/password-based sign-on experience. As a result, it significantly enhances the varied authentication management capabilities (including step-up authentication) of a CA SiteMinder WAM deployment by adding a transparent layer of strong multi-factor authentication.

Arcot RiskFort

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

Note: Arcot WebFort and Arcot RiskFort are packaged separately. For information on installation and configuration, refer to the documentation shipped with these products.

Typical Adapter Workflow

The following steps explain the procedure of user authentication and risk assessment of a transaction in the integrated solution (refer to Figure 1-1):

1. The user accesses a resource that is protected by CA SiteMinder WAM.
2. CA SiteMinder WAM performs user disambiguation by verifying to which user directory the user belongs.
3. If the authentication has to be performed by Arcot Adapter, then the Arcot Authentication Shim redirects the user to the Arcot Authentication Flow Manager.

4. The AFM guides the user through the authentication and risk evaluation process.
5. Depending on the authentication and the risk evaluation results, the Arcot State Manager saves the user's state in a token and securely communicates the authentication and risk result to the Arcot Authentication Shim.
6. The Arcot Authentication Shim, finally, evaluates and forwards the result to the CA SiteMinder WAM.

   If the user is authenticated successfully and the risk result is positive, the user is granted access to the protected resource.

What's New in this Release

The new features introduced in Arcot Adapter release 2.2 are:

- **Passing Risk Score to the SiteMinder Policy Server**

  The *Risk Score*, which is generated by Arcot RiskFort during Risk Evaluation, is set by the Authentication Shim in the SiteMinder's user repository. This Risk Score is also known as *Confidence Level* in SiteMinder and it can be used by SiteMinder during user's authorization.

  Once retrieved, the Confidence Level may then be sent to the protective application in a response (HTTP headers), used in an authorization expression, or put to some other custom use. This feature is backward compatible to support both old and new SiteMinder Policy servers.

- **Support for Arcot WebFort 6.2.1**

  The latest Arcot WebFort 6.2.1 release is supported by Arcot Adapter. This release of Arcot WebFort comes with new features such as support for partial password verification, support for ArcotOTP credentials, and OATH-based token credentials – along with other enhancements.

Note: For more information on Arcot WebFort, see the Arcot WebFort 6.2 documentation.

- **Support for Arcot RiskFort 2.2.6**

  Arcot Adapter supports the latest version of Arcot RiskFort 2.2.6 release to evaluate risk of each incoming transaction. In addition to other enhancements, this release of Arcot RiskFort includes support for SSL-based communication between the RiskFort components and the database.

	**Book:** For more information on Arcot RiskFort, see the Arcot RiskFort 2.2.6 documentation.

- **Components Name Change**

  Starting from this release, Arcot Adapter components have been renamed as listed in the following table:

  Table 1-1. Old and New Component Names

Old Component Name in Adapter 2.1 or Earlier	New Component Name in Adapter 2.2 or Later
Arcot Customization Engine (ACE)	Authentication Flow Manager (AFM)
Arcot Token Server	State Manager
CA SiteMinder Authentication Shim	Authentication Shim

  This change in the component names has resulted in a change of the file names and properties of these components. The new file names and properties are listed in Appendix B, “New File and Property Names”.

The following features were introduced in the earlier release of Arcot Adapter:

- **Integration With Backing Authentication Schemes**

  Arcot Adapter also supports backing authentication schemes that are supported by CA SiteMinder WAM. For this, the Authentication Shim acts as an interface between CA SiteMinder WAM and backing authentication scheme. It forwards the authentication requests to the backing scheme. After performing the authentication, the backing authentication scheme sends the result back to the Authentication Shim, which in turn is posted to CA SiteMinder WAM by the Authentication Shim. In this case, the adapter can just be used for risk evaluation.

- **Improved Architecture**

  The Arcot Adapter has been designed such that it can seamlessly integrated with CA SiteMinder WAM to provide strong authentication and evaluate transaction risk for CA SiteMinder WAM users. It also provides the ability to customize the authentication flows.

- **Ability to Customize Workflows**

  Arcot Adapter provides the ability to customize the authentication flows. This feature provides the CA SiteMinder WAM users the ability to use the strong, software-based authentication, and advanced risk management in conjunction with other authentication technologies supported by CA SiteMinder WAM.

- **Support for Multiple Instances of Authentication Shim**

  Arcot Authentication Shim couples the other Adapter components with the CA SiteMinder WAM. You can deploy and configure multiple instances of Authentication Shim to support multiple authentication schemes. Each instance can be used to secure different resources.

- **Support for ArcotID Client Types**

  Adapter supports all flavors (ActiveX, Flash, signed Applet and unsigned Applet) of ArcotID Client, which are used for strong authentication by WebFort.

- **Supports CA SiteMinder WAM Username-Password Authentication**

  Arcot Adapter also supports the CA SiteMinder WAM username-password authentication. This authentication can be used in conjunction with risk evaluation feature provided by RiskFort.

Chapter 2
Preparing for Installation

This chapter lists the software requirements for installing the Arcot Adapter on supported platforms and lists other prerequisites for integration. The following sections are covered in this chapter:

Software Requirements for Authentication Shim

Before proceeding with the Authentication Shim installation, ensure that the software with specific versions, as listed in the following table, is installed and configured.

Table 2-1. Software Requirements for Authentication Shim

Software	Supported Version	Supported Operating System
CA SiteMinder Policy Server	6.0 SP5 and r12.0 SP2	Solaris 10 (SPARC)
or		
CA SiteMinder Policy Server	6.0 SP5 and r12.0 SP2	Red Hat Enterprise Linux (x86) Server release 5.2 (Tikanga)

Software Requirements for FCC Pages

Before proceeding with the FCC configuration, ensure that the software with specific versions, as listed in the following table, is installed and configured.

Table 2-2. Software Requirements for FCC Pages

Software	Supported Version	Supported Operating System
CA SiteMinder Web Agent	6.0 and r12.0 SP2	Refer to CA SiteMinder WAM documentation for more information on supported operating systems.

Software Requirements for State Manager

This section discusses the following topics:

- Software Requirements
- Configuring Database Server
- Configuring the Application Server

Software Requirements

Before proceeding with the State Manager installation and deployment, ensure that the software with specific versions, as listed in the following table, is installed and configured.

Table 2-3. Software Requirements for State Manager

Software	Supported Version	Supported Operating System
Arcot RiskFort	2.2.6	Solaris 10 (SPARC)
or		
Arcot RiskFort	2.2.6	Red Hat Enterprise Linux (x86)

Book: Refer to *Chapter 3, "Preparing for Installation"* in the *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information on the software requirements for RiskFort.

Database Requirements

The following table lists the database requirements for State Manager.

Table 2-4. Minimum Database Version

Database Server
Oracle 11*g*

JDK and Application Server Requirements

The following table lists the JDK and the application server requirements for the State Manager.

Table 2-5. Minimum JDK and Application Server Version

JDK	Application Server
Sun JDK 5.0 Update 10	Apache Tomcat 5.5.23
Compatible JDK version	IBM WebSphere 6.1
Compatible JDK version	Oracle WebLogic 11gR1 or 10.3.1

Configuring Database Server

Before installing the Arcot Adapter and integrating it with CA SiteMinder, you must set up a database that is used by the State Manager.

Use the following information when setting up the database server yourself, or provide this information to your database administrator (DBA) when you request a database account.

Configuring Oracle Database

This section provides the configuration information for Oracle database.

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

Perform the following steps to setup the Oracle database:

1. Creating a New Database
2. Creating a Database User

Creating a New Database

Create a new database (recommended name is *arcotsm*) that is used to store the State Manager information.

Creating a Database User

Create a user with the following criteria:

1. Create a user (recommended name is *smadmin*), with a schema in the new database *arcotsm*.
2. Grant the user with `CONNECT` and `RESOURCE` privileges.
3. Grant the user with `CREATE TABLE` privilege.
4. Grant the user `ALTER EXTENT PARAMETERS` privilege.
5. Grant the user privileges to modify the storage extents for the `LOB` columns.

Configuring the Application Server

The State Manager is a Web application that requires a servlet container for its deployment. The State Manager uses JNDI to connect to the database, therefore you must create a JNDI connection.

It is recommended that the State Manager communicates with other components using SSL mode. To configure the State Manager for SSL, you must enable the application sever, where the State Manager is deployed for SSL communication.

Based on the application server you are using, refer to Chapter 4, “Deploying and Configuring State Manager” for details on these steps.

Software Requirements for Authentication Flow Manager

Before proceeding with the AFM deployment and configuration, ensure that the software with specific versions, as listed in the following table, is installed and configured.

Table 2-6. Software Requirements for AFM

Software	Supported Version	Supported Operating System
Arcot WebFort	6.2.1	Solaris 10 (SPARC)
or		
Arcot WebFort	6.2.1	Red Hat Enterprise Linux (x86)

Book: Refer to *Chapter 3, "Preparing for Installation"* in the *Arcot WebFort 6.2 Installation and Deployment Guide* for more information on the software requirements for WebFort.

JDK and Application Server Requirements

The following table lists the JDK and the application server requirements for the AFM.

Table 2-7. Minimum JDK and Application Server Version

JDK	Application Server
Sun JDK 5.0 Update 10	Apache Tomcat 5.5.23
Compatible JDK version	IBM WebSphere 6.1
Compatible JDK version	Oracle WebLogic 11gR1 or 10.3.1

Prerequisites for Integration

The following requirements must be met before proceeding with the integration:

- At least two instances of application servers are running.
- Required number of database instances are ready with applicable schemas.
- Arcot WebFort 6.2.1 is installed on the required operating system.

Book: Refer to *Arcot WebFort 6.2 Installation and Deployment Guide* for installation details.

- Arcot RiskFort 2.2.6 is installed on the required operating system.

Book: Refer to *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for installation details.

- SiteMinder Policy Server and SiteMinder Web Agent are installed and configured.

  Refer to the appropriate SiteMinder documentation for installation details.

- You must create at least one object of the following elements using SiteMinder Administration tool. Refer to the appropriate SiteMinder documentation for more information on creating these objects:
  - Agents
  - Domains
  - Administrators
  - Realms
  - Users
  - User directories
  - Rules for the realms

Chapter 3
Installing Arcot Adapter

This chapter provides instructions for installing the Arcot Adapter. On successfully completing the installation process, you can configure CA SiteMinder WAM to make use of the multi-factor ArcotID authentication and the risk-based adaptive authentication provided by Arcot Adapter. This chapter covers the following topics:

Note: If you are installing Arcot Adapter and other Arcot products on the same system in the same location, then other Arcot products *must* be installed *before* installing the Arcot Adapter.

Installing Arcot Adapter

The **Arcot Adapter InstallAnywhere Wizard** is used to install the Adapter components. You need to follow the instructions in the InstallAnywhere Wizard, which will guide you to extract and install the required Adapter components on your system. For integrating Arcot Adapter with CA SiteMinder WAM, you *need* to install the following components: Authentication Flow Manager, State Manager, Authentication Shim, Form Credential Collector pages, and the scripts required for setting up the database that you intend to use for the Adapter.

Important: Before proceeding with the installation, ensure that all prerequisite software components are installed and the database is set up, as described in Chapter 2, “Preparing for Installation”.

Perform the following steps to install the Arcot Adapter:

1. Log in to the operating system.
2. Create a temporary directory using the following command:

```
prompt> mkdir /tmp_install
```

3. Copy the installer GZIP file to the temporary directory that you created in Step 2:
   - **For Solaris:**

     ```
     prompt> cp Arcot-Adapter-2.2-Solaris.tar.gz /tmp_install
     ```
   - **For Linux:**

     ```
     prompt> cp Arcot-Adapter-2.2-Linux.zip /tmp_install
     ```
4. Unzip the installer file as shown in the following commands:
   - **For Solaris:**

     ```
     prompt> cd /tmp_install
     prompt> gzip –d Arcot-Adapter-2.2-Solaris.tar.gz
     ```
   - **For Linux:**

     ```
     prompt> cd /tmp_install
     prompt> unzip Arcot-Adapter-2.2-Linux.zip
     ```
5. (*For Solaris*) Extract the TAR file, using the following command:

   ```
   prompt> tar –xvf Arcot-Adapter-2.2-Solaris.tar
   ```
6. (*For Solaris*) Navigate to the directory where you untarred the installer and run the following command to grant execute permissions to the installer file:

   ```
   prompt> chmod a+x Arcot-Adapter-2.2-Solaris-Installer.bin
   ```
7. Run the installation wizard by using the following command:

   ```
   prompt> sh Arcot-Adapter-2.2-<platform name>-Installer.bin
   ```

Note: If you are installing Adapter as a `root` user, the following warning message appears:

```
You are installing as "root".

Do you want to continue with the installation? (Y/N):.
```

Enter **Y** or **y** to continue.

The installer starts preparing for the installation and the Welcome screen appears.

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

   The License Agreement for Arcot Adapter appears.

9. Read the agreement and press **Enter** until the license agreement is complete.

   At the end of the license agreement, the user is prompted for the confirmation.

10. Enter **Y** *or* **y** to accept the terms of the license agreement and press **Enter** to continue with the installation.

    The Choose Installation Location screen appears.

11. Enter the absolute path of the directory where the installation has to be performed. Else, press **Enter** to use the default path.

Note: The installation directory name that you specify must not contain any spaces. Doing so might result in Adapter scripts and tools functionality failure.

    The Choose Installation Type screen appears.

12. Select the type of installation:

    - **Complete**: Select this option if you want to install *all* components of Arcot Adapter on the current system.
    - **Customize**: Select this option if you want to install only *selected* components of Arcot Adapter on the current system. In this case, you need to install the remaining components on other system(s).

13. Press **Enter** to continue.

    If you selected Complete, then proceed to Step 15.

    If you selected Customize, then the Choose Installation Components screen appears.

14. (*Custom Installation Only*) By default, all components are selected for installation. Enter the number of the components (separated by a comma) that you *do not* want to install on the current system.

The following table lists the components that you can install:

Table 3-1. Arcot Adapter Components

Components	Description
1- Authentication Flow Manager	The Authentication Flow Manager (AFM) navigates the user through the authentication process, risk evaluation process, or both.
2- State Manager	The Arcot State Manager generates, maintains, and tracks the tokens that are used to associate the authentication and risk status of the user's session across Arcot Adapter and CA SiteMinder WAM components.
3- Authentication Shim	The Authentication Shim is the core component that enables interaction between Arcot components, CA SiteMinder WAM, and other authentication schemes.
4- Form Credential Collector Pages	The FCC pages collect authentication input from the user and send it for authentication and risk evaluation.

15. Press **Enter** to continue.

    The Pre-Installation Summary screen appears.

    Review the information on this screen, if you need to change a previous selection, then type `back` to go back to the previous installation step and make the required changes.

16. On the Pre-Installation Summary screen, press **Enter** to continue.

    The Ready to Install screen appears.

17. Press **Enter** to begin the installation process.

    The Installing screen appears, which would start installing the selected components on your system.

Note: The installation process might take some time to complete.

On successful installation, the Installation Complete screen appears.

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

Note: If for some reason, the installation failed, the error log is available in the same location where you ran the Installer from.

Configuring Adapter for Silent Mode Installation

The Arcot Adapter installer can be customized to run in the *Silent Mode*, which does not require any user interaction to install the application. As an administrator, you record the response to the information required by the installer in a separate file–also known as the *response file*– and ship this file along with the installer. After you have created the response file, all that is required to complete the installation process on a different system is to launch the `Arcot-Adapter-2.2-<platform name>-Installer.bin` file.

To prepare Arcot Adapter installer to run in the silent mode, perform the following steps:

1. Log in to the operating system.
2. Create a temporary directory using the following command:

   ```
   prompt> mkdir /tmp_install
   ```

3. Copy the installer GZIP file to the temporary directory that you created in Step 2:
   - **For Solaris:**

     ```
     prompt> cp Arcot-Adapter-2.2-Solaris.tar.gz /tmp_install
     ```

   - **For Linux:**

     ```
     prompt> cp Arcot-Adapter-2.2-Linux.zip /tmp_install
     ```

4. Unzip the installer file as shown in the following commands:
   - **For Solaris:**

     ```
     prompt> cd /tmp_install
     prompt> gzip –d Arcot-Adapter-2.2-Solaris.tar.gz
     ```

- **For Linux:**

```
prompt> cd /tmp_install
prompt> unzip Arcot-Adapter-2.2-Linux.zip
```

5. (*For Solaris*) Extract the TAR file, using the following command:

   ```
   prompt> tar –xvf Arcot-Adapter-2.2-Solaris.tar
   ```

6. (*For Solaris*) Navigate to the directory where you untarred the installer and run the following command to grant execute permissions to the installer file:

   ```
   prompt> chmod a+x Arcot-Adapter-2.2-Solaris-Installer.bin
   ```

7. Create a response file by running the installer using the following command:

   ```
   prompt> sh Arcot-Adapter-2.2-<platform name>-Installer.bin -r
           /tmp_install/installer.properties
   ```

   Executing this command would start the Adapter's installation process. You need to complete the installation process by providing the information required by the installer. The response you provide during the installation process is stored in the `installer.properties` file.

8. Open the `installer.properties` file in a text editor and change the following two properties as:

   ```
   INSTALLER_UI=Silent
   CHOOSE_INSTALL_DIR=<Install_Location_for_Arcot_Adapter>
   ```

   Save and close the `installer.properties` file.

9. Repackage the Adapter's installation file along with the response file–`installer.properties`.

Note: Before repackaging, ensure that the `Arcot-Adapter-2.2-<platform name>-Installer.bin` and `installer.properties` files are stored in the same location.

To install Arcot Adapter in Silent Mode:

1. Navigate to the directory where the `Arcot-Adapter-2.2-<platform name>-Installer.bin` file is located.
2. Run the installation wizard by executing the following command:

   ```
   prompt> sh Arcot-Adapter-2.2-<platform name>-Installer.bin
   ```

   The installer runs as a background process without requiring any user interaction.
3. To verify whether the installation process has completed successfully, look for the directory that was specified in the `CHOOSE_INSTALL_DIR` parameter.

Installation Logs

After installation, you can access the installation log file – **`Arcot_Adapter_2.2_InstallLog.log`** from the following directory:
`<installation_dir>/`**`logs/`**

Note: `<installation_dir>` is the directory where the Adapter is installed. By default, it is installed in the `/opt/`**`arcot`** directory.

Installation Directory

Arcot Adapter installs the directories and files listed in the following table.

Important: In addition to the directories and files discussed in Table 3-2, you will also see **`arcotkey`** and **`adapterkey`** files in the **`arcot`** directory. These files are used by the installer to detect any previously installed Arcot product. If these files are deleted, the installer will not be able to detect if any Arcot product was previously installed. As a result, it will allow new installations to be performed in any location and will not be able to ensure the same destination directory for multiple Arcot products. In such cases, the products might not work, as expected. However, these files have no impact on patches and upgrade.

Table 3-2. Arcot Adapter Directory Structure

Component	Location	Files
Authentication Shim	<*installation_dir*>/adapterSiteMinder/certs	Contains the default root CA certificate, client certificate, and client key files in .PEM format. **Note:** These certificates are bundled with the package for testing purpose only. You can use these files to enable two-way SSL communication between the Authentication Shim and the State Manager.
	<*installation_dir*>/adapterSiteMinder/lib	Contains the following files: • ArcotLog2FileSC.so: Log library file • libArcotSiteMinderAdapter.so: Authentication Shim library file.
FCC Pages	<*installation_dir*>/adapterSiteMinder/fcc	Contains the Form Credential Collector (FCC) pages and **js** directory, which contains the JavaScript files. The **fcc** directory contains the following files: • shim.fcc This page accepts username and LDAP password as input for authenticating the user. This FCC page is used in One-Page login scenario. • shim2.fcc This page accepts username, which is used for further processing. This FCC page is used in Two-Page login scenario. In this scenario, the LDAP password is collected by shimfinal2.fcc page. In addition, this page also collects the username when the authentication, risk evaluation, or both are performed by the Authentication Shim. • shimerror.fcc This page is displayed if any error occurs during authentication. • shimfinal.fcc This page is used by the AFM to redirect the user back to Policy Server after authentication, risk evaluation, or both based on the authentication flow.

Table 3-2. Arcot Adapter Directory Structure

Component	Location	Files
		• `shimfinal2.fcc` This page collects the LDAP password of the user to authenticate the user. It is used in Two-Page login scenario where the SiteMinder authentication is performed after the risk evaluation. • `shimunknownuser.fcc` This page is displayed if you access the FCC pages directly and not as a result of redirection. • `shimerror.unauth.html` This page is displayed if the user enters incorrect username or password more than maximum attempts that are allowed by SiteMinder.
State Manager	`<installation_dir>/adapterStateManager`	Contains WAR, JDBC drivers, properties files, and keystores required by the State Manager. Contains the following subdirectory: • `certs` Contains the keystore and truststore files required by the State Manager. **Note:** These keystore and truststore files are bundled with the package for testing purpose only. You can use these files to enable two-way SSL communication between the State Manager, Authentication Shim, and AFM.
Authentication Flow Manager	`<installation_dir>/adapterAFM`	Contains the WAR and properties files used by the AFM. Contains the following subdirectory: • `certs` Contains the keystore and truststore files required by the AFM. **Note:** These keystore and truststore files are bundled with the package for testing purpose only. You can use these files to enable two-way SSL communication between the AFM and State Manager.

Table 3-2. Arcot Adapter Directory Structure

Component	Location	Files
Common Files and Directories Created by Adapter	`<installation_dir>/conf`	Contains the `adaptershim.ini` file that contains the Authentication Shim configuration parameters.
	`<installation_dir>/docs`	Contains the Java documents for AFM tasks.
	`<installation_dir>/ext-license`	Contains the licenses of the third-party software that are used with Adapter.
	`<installation_dir>/dbscripts`	Contains the SQL scripts required to create the State Manager schema in the supported database. Contains the following subdirectories: • `oracle` Contains the SQL scripts for creating database schema in the Oracle database server.
	`<installation_dir>/Uninstall_Arcot Adapter 2.2`	Contains the files required for uninstalling the Adapter.
	`<installation_dir>/logs`	Contains the installation and Authentication Shim log files. Contains the following subdirectory: • `backup` Stores the rolled over log files of the Authentication Shim.

Chapter 4
Deploying and Configuring State Manager

This chapter provides the details that are required to successfully deploy and configure the State Manager. It covers the following topics:

Note: Before deploying and configuring the State Manager, ensure that the RiskFort Server is started and running.

Copying the JDBC Drivers

State Manager connects to the database by using a JDBC connection. The Adapter installation package provides the JDBC drivers that the State Manager uses.

If you are using Apache Tomcat to deploy the State Manager, then you can use these drivers. If you are using IBM WebSphere or Oracle WebLogic to deploy the State Manager, you can use either the default drivers that are shipped with the application server or the drivers that are provided with Adapter.

Copy the following driver:

For Oracle Database:

`ojdbc14.jar`

from
`<installation_dir>/adapterStateManager/`

Note: `<installation_dir>` is the directory where the Adapter is installed. By default, it is installed in the `/opt/arcot` directory.

to
`<Tomcat_root>/common/lib/`

Note: `<Tomcat_root>` refers to the the Apache Tomcat installation directory.

Running Database Scripts

Note: Before you run the scripts discussed in this section, you must ensure that you are logged in as the same database user that you created in the section "Configuring Database Server" in Chapter 2.

Arcot Adapter is shipped with scripts that are required to create necessary tables in the database.

To create the required database tables:

1. Navigate to the following location:

   For Oracle:

   `<installation_dir>/dbscripts/oracle`

2. If you are using a single database for all Arcot products, then open the `arcot-db-config-for-adapter-statemanager-2.2.sql` file in a text editor and execute *only* the `CREATE TABLE ARTSTOKENS` command in the database. This would create only a single table in your database – `ARTSTOKENS`.

   or

If you are using separate database for Arcot Adapter, then execute the **arcot-db-config-for-adapter-statemanager-2.2.sql** script to create the database tables. This would create two tables in your database – **ARTSTOKENS** and **ARCMNDBERRORCODES**

ARTSTOKENS table contains the token information, such as the token ID, time when the token was issued and last used, and the timestamp of communication with RiskFort. The **ARCMNDBERRORCODES** table contains the database error codes.

Creating a JNDI Connection

This section describes the steps to create the JNDI connection on the following application servers that are supported by State Manager:

- On Apache Tomcat
- On IBM WebSphere
- On Oracle WebLogic

Note: The following subsections describe the steps for creating JNDI connections for the primary database server. If database failover support is needed, then you would also need to specify the data sources with JNDI names for the secondary database server(s).

On Apache Tomcat

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

1. Ensure the Apache Tomcat application server is installed and functional.
2. Create a new file as – **arcotsm.xml** to specify the JNDI data source and copy it to the following directory:

   <Tomcat_root>/conf/Catalina/localhost

   For Apache Tomcat 5.5.x and Oracle database:
3. Open the arcotsm.xml file and add the following code:

```
<Context path="/arcotsm" docBase="arcotsm"
debug="5" reloadable="true" crossContext="true">
```

```
<Resource name="jdbc/ArcotStateManagerDataSource1" auth="Container"
type="javax.sql.DataSource"
maxActive="100" maxIdle="30" maxWait="30000"
driverClassName="oracle.jdbc.driver.OracleDriver"
username="smadmin" password="123456"
url="jdbc:oracle:thin:@<host>:<port>:<sid>"/>
</Context>
```

4. Replace the following parameters in the `Context -> Resource` section.

Table 4-1. Configuration Parameters

Parameter	Replace With
`username`	Logon identifier of the database user.
`password`	Logon password of the database user.
`url`	Change the `host`, `port`, and `SID` information in the `url` parameter to that of the database server.

5. Save and close the `arcotsm.xml` file.

On IBM WebSphere

In the IBM WebSphere Management Console, use the **Resources** -> **JDBC Node** option to create a data source with the JNDI name as `jdbc/ArcotStateManagerDataSource1`.

On Oracle WebLogic

In the Oracle WebLogic Administration Console, use **Services** -> **JDBC** -> **Data Sources** option to create a data source with the JNDI name as `jdbc/ArcotStateManagerDataSource1`.

Deploying State Manager

Note: If you choose to deploy the State Manager at this point, then you need to follow the *Method 1* to edit the properties files as explained in the sections, "Editing the State Manager Properties File" and "Editing the Log Properties File".

If you choose to skip the deployment process, then you need to follow the *Method 2* for editing the properties file.

You need the **arcotsm.war** file to deploy the State Manager. This file is available at the following location:

`<installation_dir>/adapterStateManager/`

Important: If you have used Arcot Adapter 2.1 or earlier, see Appendix B, "New File and Property Names" for information on the file names and properties that have been renamed in Arcot Adapter 2.2 release.

To deploy the State Manager:

1. Install `arcotsm.war` on the application server.

   For example, on Apache Tomcat the location to install the `WAR` file is as follows:

   `<application_server_home>/webapps`

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

2. Restart the application server.

   The application server must now contain a directory – `arcotsm`.

Enabling SSL

Arcot recommends that you enable the State Manager to communicate with the other components using SSL. For this, you must enable the application server where the State Manager is deployed for SSL communication. Refer to the documentation of your application server for more information on this. For testing purpose, you can use the default certificates shipped with the Arcot

Adapter package to enable the SSL communication between the Adapter components. For more information on the location of these test certificates, see the directory structure of the State Manager.

Editing the State Manager Properties File

You can choose any of the following method to edit the State Manager's properties file:

- Method 1: use this method if you have *already deployed* the State Manager.
- Method 2: use this method if you have *not deployed* the State Manger.

Method 1

Perform the following steps to edit the **`arcotsm.properties.src`** file, which is available in the following directory:

Note: The location mentioned here is specific to Apache Tomcat. If you are using other application severs, refer to the application server's documentation for corresponding path.

`<application_server_home>/webapps/arcotsm/WEB-INF/classes/`

1. Make a copy of `arcotsm.properties.src` file in the same directory and rename it to **`arcotsm.properties`**.
2. Edit the `arcotsm.properties` file in a text editor and configure the RiskFort parameters as described in the following table.

Table 4-2. RiskFort Configuration Parameters

Parameter	Required/ Optional	Description
`RiskFortHOST.1`	Required	Specify the IP address or the *Fully Qualified Distinguished Name* (FQDN) of the RiskFort Server.
`RiskFortPORT.1`	Required	Specify the port where RiskFort Server is listening to the incoming requests. Default value: **`7680`**

Table 4-2. RiskFort Configuration Parameters

Parameter	Required/ Optional	Description
`RiskFortTRANSPORT_TYPE`	Optional	Specify the protocol for the RiskFort Server to start up. **Note:** It is highly recommended that State Manager communicates with RiskFort using SSL. Refer to *Arcot RiskFort 2.2.6 Installation and Deployment Guide* for more information on how to configure RiskFort for SSL. Default value: **`TCP`**
`RiskFortCA_CERT_FILE`	Required, *if* `RiskFortTRANSPORT_TYPE=SSL`	Provide the *complete path* of the CA certificate file for the RiskFort Server. The file *must* be in `.PEM` format.
`RiskFortCLIENT_P12_FILE`	Required, *if* `RiskFortTRANSPORT_TYPE=SSL`	Provide the path of the PKCS 12 file that contains the key and certificate of client communicating with the RiskFort Server. This would establish two-way SSL between the RiskFort client and server.
`RiskFortCLIENT_P12_PASSWORD`	Required, *if* `RiskFortTRANSPORT_TYPE=SSL`	Provide the password to open the PKCS 12 file specified in the `RiskFortCLIENT_P12_FILE` parameter.
`RiskFortCONNECTION_TIMEOUT`	Optional	Specify the time (in milliseconds) before the RiskFort Server is considered unreachable. Default value: **`30000`** *`(30 seconds)`*
`RiskFortREAD_TIMEOUT`	Optional	Specify the maximum time (in milliseconds) allowed for a response from the RiskFort Server. Default value: **`30000`** *`(30 seconds)`*
`RiskFortCONNECTION_RETRIES`	Optional	Specify the maximum number of retries allowed to connect to the RiskFort Server. Default value: **`3`**

Table 4-2. RiskFort Configuration Parameters

Parameter	Required/ Optional	Description
`RiskFortUSE_CONNECTION_POOLING`	Optional	Specify whether the connection pooling with the RiskFort Server is enabled or disabled. Default value: **`1`** (*enabled*)
`RiskFortMAX_ACTIVE`	Optional	Specify the number of maximum connections that can exist between the State Manager and RiskFort Server. At any given instance, the number of connections cannot exceed this value. Default value: **`32`**
`RiskFortTIME_BETWEEN_CONNECTION_EVICTION`	Optional	Specify the time (in milliseconds) after which the connection eviction thread will be executed to check and delete any idle RiskFort Server connection. Default value: **`900000`** *`(90 seconds)`*
`RiskFortIDLE_TIME_OF_CONNECTION`	Optional	Specify the time (in milliseconds) after which an idle RiskFort Server connection will be dropped. Default value: **`1800000`** *`(3 minutes)`*
`RiskFortWHEN_EXHAUSTED_ACTION`	Optional	Specifies the behavior when the maximum number of supported connections have exhausted. Default value: **`BLOCK`**

3. Configure the token-related parameters, which are described in the following table.

Table 4-3. Token Configuration Parameters

Parameter	Required/ Optional	Description
`TokenMaxInactivitySeconds`	Optional	Specify the time (in seconds) for which the token can be idle after an operation is performed on it. If there is no action on the token within this period, the token becomes unusable. Default value: **`300`** *`(5 minutes)`*
`TokenMaxLifetimeSeconds`	Optional	Specify the maximum amount of time (in seconds) the token is accessible after it is generated. Default value: **`900`** *`(15 minutes)`*

Table 4-3. Token Configuration Parameters

Parameter	Required/ Optional	Description
`TokenCleanupIntervalSeconds`	Optional	Specify the frequency (in seconds) at which the expired tokens are checked and deleted from the database. Default value: **`30`**
`TSMClass`	Optional	Specify the type of storage mechanism to be used for the State Manager, which is a JDBC database. Default value: **`com.arcot.integrations.toksvr.server.tsmimpl.iBatisTSMImpl`**

4. Configure the database connectivity parameters, which are described in the following table.

Table 4-4. Database Connectivity Parameters

Parameter	Required/ Optional	Description
`DbType`	Required	Specify the type of the database applicable to all database connections. As this parameter does not have any default value, you need to uncomment and specify the applicable database type, which should be set to `oracle`.
`AutoRevert`	Optional	Specifies whether or not the system attempts to reconnect to the primary database after a failover occurs. Set `AutoRevert=1`, if you have a backup database configured and if you want the server to reconnect to the primary database after it has switched to the backup database. Default value: **`1`**

Table 4-4. Database Connectivity Parameters

Parameter	Required/ Optional	Description
`AppServerConnectionPoolName.<n>`	Required	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 State Manager for it to use the connection pool. For example, configure this property as: `AppServerConnectionPoolName.1=java:comp/env/jdbc/ArcotStateManagerDataSourceName`

5. To enforce a secure communication between the State Manager and other components, ensure that the parameter `RequireSecureConnection` is set to `true`, which is also the default value.
6. Proceed with log properties file configuration using the "Method 1" as described in the section, "Editing the Log Properties File".

Method 2

Adapter installs the `arcotsm.properties` file on the file system, you can also use this file to edit the required parameters by performing the following steps:

1. Open the `arcotsm.properties` file, which is available in the following directory:

   `<installation_dir>/adapterStateManager/`
2. Edit the file parameters as described in Step 2 to Step 5.
3. Proceed with log properties file configuration using the "Method 2" as described in the section, "Editing the Log Properties File".

Editing the Log Properties File

You can choose any of the following method to edit the State Manager's log properties file:

- Method 1: use this method if you have *already deployed* the State Manager.
- Method 2: use this method if you have *not deployed* the State Manger.

Method 1

Perform the following steps to edit the **log4j.properties.src** file, which is available in the following directory:

Note: The location mentioned here is specific to Apache Tomcat. If you are using other application severs, refer to the application server's documentation for corresponding path.

`<application_server_home>/webapps/arcotsm/WEB-INF/classes/`

1. Make a copy of `log4j.properties.src` file in the same directory and rename it to **log4j.properties**.
2. Edit the `log4j.properties` file to set the log file information as described in the following table.

Table 4-5. Log Configuration Parameters

Parameter	Description
`log4j.appender.smlog.File`	Specify the log file name and the location where the State Manager logs must be written to. By default, the State Manager log file name is `arcotsm.log` and it is created in the `<application_server_home>/`**logs** directory.

Method 2

Adapter installs the `log4j.properties` file on the file system, you can also use this file to edit the required parameters by performing the following steps:

1. Open the `log4j.properties` file, which is available in the following directory:

   `<installation_dir>/adapterStateManager/`
2. Edit the file parameter as described in Table 4-5.
3. Create `arcotsm.war` with the edited `arcotsm.properties` and `log4j.properties` files.
4. Deploy the `arcotsm.war` file on the application server.

Testing the Configuration

To test the State Manager configuration:

1. Restart the application server.
2. Access the State Manager using the following URL:

   https://<Host>:<Port>/arcotsm/index.jsp
3. Open the State Manager log file from the location you have configured it in the `log4j.properties` file. By default, the log file is available in the following directory:

   For Apache Tomcat 5.5

   <application_server_home>`/logs`
4. Search for the following lines in the log file, which indicates that the State Manager is configured successfully.

```
Servlet com.arcot.integrations.toksvr.server.TokenCreator starting up
Servlet com.arcot.integrations.toksvr.server.TokenReader starting up
Servlet com.arcot.integrations.toksvr.server.TokenRemover starting up
```

Chapter 5
Deploying and Configuring Authentication Flow Manager

This chapter lists the tasks that you must perform to deploy and configure the Authentication Flow Manager (AFM) successfully. It covers the following topics:

- Deploying Authentication Flow Manager
- Enabling SSL
- Editing the Authentication Flow Manager Properties File
- Editing the Log Properties File
- Testing the Configuration

Note: Before deploying and configuring the AFM, ensure that the WebFort Server is started and running.

Deploying Authentication Flow Manager

Note: If you choose to deploy the AFM at this point, then you need to follow the *Method 1* to edit the properties files as explained in the sections, "Editing the Authentication Flow Manager Properties File" and "Editing the Log Properties File".

If you choose to skip the deployment process, then you need to follow the *Method 2* for editing the properties file.

You need the `arcotafm.war` file to deploy the AFM. This file is available at the following location:

`<installation_dir>/adapterAFM/`

Important: If you have used Arcot Adapter 2.1 or earlier, see Appendix B, "New File and Property Names" for information on the file names and properties that have been renamed in Arcot Adapter 2.2 release.

To deploy the AFM application:

1. Install `arcotafm.war` on the application server.

   For example, on Apache Tomcat the location to install the `WAR` file is:

   `<application_server_home>/webapps`

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

2. Restart the application server.

   The application server should now contain a directory – `arcotafm`.

Enabling SSL

Arcot recommends that you enable the AFM to communicate with the other components using SSL. For this, you must enable the application server where the AFM is deployed for SSL communication. Refer to the documentation of your application server for more information on this. For testing purpose, you can use the default certificates shipped with the Arcot Adapter package to enable the SSL communication between the Adapter components. For more information on the location of these test certificates, see the directory structure of the Authentication Flow Manager.

Editing the Authentication Flow Manager Properties File

You can choose any of the following method to edit the AFM properties file:

- Method 1: use this method if you have *already deployed* the AFM.
- Method 2: use this method if you have *not deployed* the AFM.

Method 1

Perform the following steps to edit the **`arcotafm.properties.src`** file, which is available in the following directory:

Note: The location mentioned here is specific to Apache Tomcat. If you are using other application severs, then refer to the application server's documentation for corresponding path.

`<application_server_home>/webapps/arcotafm/WEB-INF/classes/`

1. Make a copy of this file in the same directory and rename it to `arcotafm.properties`.
2. Edit the `arcotafm.properties` file in a text editor and configure the State Manager's parameters as described in the following table.

Table 5-1. State Manager Configuration Parameters

Parameter	Required/ Optional	Description
`ArcotAFMLandingURL`	Optional	Provide the URL of the Authentication Flow Manager's controller JSP. The controller JSP depends on the authentication flow. This is an optional overriding parameter for Landing URL.
`ArcotSMHostname`	Required	Specify the *Fully Qualified Distinguished Name* (FQDN) or IP address of the State Manager.
`ArcotSMPort`	Required	Specify the port of the application server at which the State Manager is deployed.
`ArcotSMBaseURL`	Optional	Specify the path where the State Manager is available. Default value: **`arcotsm/servlet`**
`ArcotSMSecureConnection`	Optional	Specify whether the AFM communicates with the State Manager in a secure mode over SSL. Possible values: • `true` • `false` Default value: **`true`**

Table 5-1. State Manager Configuration Parameters

Parameter	Required/ Optional	Description
`ArcotSMTrustStore`	Optional	Specify the path where the root SSL certificate of the server is present. This parameter is valid if `ArcotSMSecureConnection` is set to `true`. Default value: **`/certs/tsclient.truststore`**
`ArcotSMTrustStorePassword`	Optional	Specify the password of the truststore. This parameter is valid if `ArcotSMTrustStore` path is provided.
`ArcotSMKeyStore`	Optional	Specify the path of the client SSL keystore. Default value: **`/certs/tsclient.keystore`**
`ArcotSMKeyStorePassword`	Optional	Specify the password of the keystore.
`ArcotSMConnTimeoutMS`	Optional	Specify the interval (in milliseconds) to open a connection with the State Manager. If no response is received within the specified time frame, the connection is dropped. Default value: **`15000`** *(15 seconds)*
`ArcotSMReadTimeoutMS`	Optional	Specify the period (in milliseconds) for which the AFM must wait for the response from the State Manager. Default value: **`30000`** *(30 seconds)*
`ArcotSMMaxRetries`	Optional	Specify the maximum number of retries allowed to connect to State Manager. Default value: **`0`** *(no retries)*
`ArcotSMTestConnAtStartup`	Optional	Specify if a test token must be created when the Web application is being started. **Note:** If you are using JRE 1.4.2.x and the AFM starts before the State Manager, then AFM cannot time-out the connection, and it does not start up. Possible values: • `true` • `false` Default value: **`true`**

3. Configure the WebFort Server's authentication parameters, which are described in the following table.

Table 5-2. WebFort Configuration Parameters

Parameter	Required/ Optional	Description
`WebFortauthentication.host.1`	Required	Specify the FQDN or IP address of the WebFort Server.
`WebFortauthentication.port.1`	Required	Specify the port at which the WebFort Server is available. Default value: **`9742`**
`WebFortauthentication.transport.1`	Optional	Specify the protocol for the WebFort Server to start up. **Note:** It is highly recommended that AFM communicates with WebFort using SSL. Refer to *Arcot WebFort 6.2 Installation and Deployment Guide* for more information on how to configure WebFort for SSL. Default value: **`TCP`**
`WebFortauthentication.serverCACertPEMPath.1`	Required, *if* `WebFortauthentication.transport.1=SSL`	Provide the *complete path* of the *certification authority* (CA) certificate file for the WebFort Server. The file *must* be in `.PEM` format.
`WebFortauthentication.clientCertKeyP12Path.1`	Required, *if* `WebFortauthentication.transport.1=SSL`	Provide the path of the `p12` file that contains the key and certificate of client communicating with the WebFort Server. This would establish two-way SSL between the WebFort client and server.
`WebFortauthentication.clientCertKeyPassword.1`	Required, *if* `WebFortauthentication.transport.1=SSL`	Provide the client key pair password to open the `p12` file specified in the `WebFortauthentication.clientCertKeyP12Path.1` parameter.

Table 5-2. WebFort Configuration Parameters

Parameter	Required/ Optional	Description
`WebFortpool.maxactive`	Optional	Specify the maximum number of connections that can exist between the AFM and WebFort Server. At any given instance, the number of connections cannot exceed this value. Default value: **32**
`WebFortpool.maxIdle`	Optional	The maximum number of idle connections allowed in the pool from the SDK to the WebFort Server. Default value: **16**
`WebFortpool.maxWaitTimeMillis`	Optional	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. Default value: **-1**
`WebFortpool.minEvictableIdleTimeMillis`	Optional	The minimum amount of time a connection might be idle in the pool before it is evicted by the idle connection evictor, if any. Default **-1** indicates that the idle connection would not be evicted. Default value: **-1**
`WebFortpool.timeBetweenEvictionRunsMillis`	Optional	The amount of time (in milliseconds) to sleep before checking the pool to evict the idle connections. Default **-1** indicates that the there would not be any connection eviction. Default value: **-1**
`WebFortauthentication.connectionTimeout.1`	Optional	Specify the time (in milliseconds) before the WebFort Server is considered unreachable. Default value: **10000** *(10 seconds)*
`WebFortauthentication.readTimeout.1`	Optional	Specify the maximum time (in milliseconds) allowed for a response from the WebFort Server. Default value: **30000** *(30 seconds)*

4. Configure the User Browser Resources parameters, which are described in the following table.

Table 5-3. User Browser Resources Parameters

Parameter	Required/ Optional	Description
`DeviceIDType`	Optional	Specify the type of cookie that must be stored on the end-user's system. RiskFort uses Device ID to register and identify the device that is used by a user during transactions. The Device ID needs to be set as a cookie on the user's computer. This cookie can either be an HTTP cookie or a Flash cookie. Possible values: • `httpcookie` • `flashcookie` Default value: **`httpcookie`**
`ClientType1`	Optional	Specify the ArcotID Client type that must be used when an ArcotID authentication is performed by WebFort. Possible values: • `Flash` • `ActiveX` • `Applet` • `UnsignedApplet`
`ClientType2`	Optional	Specify the client type to be used for authentication. If ArcotID Client type specified in the `ClientType1` parameter is not available, the Arcot Adapter checks this parameter for which client to use. Possible values: • `Flash` • `ActiveX` • `Applet` • `UnsignedApplet`

Table 5-3. User Browser Resources Parameters

Parameter	Required/ Optional	Description
`ClientType3`	Optional	Specify the client type to be used for authentication. If ArcotID Client type specified in the `ClientType1` and `ClientType2` parameters is not available, the Arcot Adapter checks this parameter for which client to use. Possible values: • `Flash` • `ActiveX` • `Applet` • `UnsignedApplet`

5. Proceed with log properties file configuration using the "Method 1" as described in the section, "Editing the Log Properties File".

Method 2

The Adapter installs `arcotafm.properties` on the file system, you can also use this file to edit the required parameters by performing the following steps:

1. Open the `arcotafm.properties` file, which is available in the following directory:

   `<installation_dir>/adapterAFM/`

2. Edit the file parameters as described in Step 2 to Step 4.
3. Proceed with log properties file configuration using the "Method 2" as described in the section, "Editing the Log Properties File".

Editing the Log Properties File

You can choose any of the following method to edit the AFM's log properties file:

- Method 1: use this method if you have *already deployed* the AFM.
- Method 2: use this method if you have *not deployed* the AFM.

Method 1

Perform the following steps to edit the **`log4j.properties.src`** file, which is available in the following directory:

Note: The location mentioned here is specific to Apache Tomcat. If you are using other application severs, refer to the application server's documentation for corresponding path.

`<application_server_home>/webapps/arcotafm/WEB-INF/classes/`

1. Make a copy of this file in the same directory and rename it to `log4j.properties`.
2. Edit the `log4j.properties` file to set the log file information as mentioned in the following table.

Table 5-4. Log Parameters

Parameter	Description
`log4j.appender.afmout.File`	Specify the log file name and the location where the AFM logs must be written to. By default, the AFM log file name is `arcotafm.log` and is created in the *`<application_server_home>`*`/logs` directory.

Method 2

The Adapter installs the `log4j.properties` file on the file system, you can also use this file to edit the required parameters by performing the following steps:

1. Open the `log4j.properties` file, which is available in the following directory:

   `<installation_dir>``/adapterAFM/`

2. Edit the file parameters as described in Table 5-4.
3. Create `arcotafm.war` with the edited `arcotafm.properties` and `log4j.properties` files.
4. Deploy the `arcotafm.war` file on the application server.

Testing the Configuration

To test the Authentication Flow Manager configuration:

1. Restart the application server.
2. Open the AFM log file from the location you have configured it in the `log4j.properties` file. By default, the log file is available in the following directory:

   For Apache Tomcat 5.5

   `<application_server_home>/logs`
3. Search for the following lines in the log file, which indicates that the AFM is configured successfully.

```
InitializeTokenSvrClientServlet for Adapter Authentication Flow
Manager version 2.2
WebFort connection test successful
```

Chapter 6
Configuring Authentication Shim and FCC Pages

This chapter provides the details that are required to successfully configure the Form Credential Collector (FCC) pages and Authentication Shim. This chapter covers the following topics:

- Deploying FCC Pages
- Deploying Authentication Shim
- Enabling SSL
- Configuring Shim
- Testing the Configuration

Deploying FCC Pages

To deploy the FCC pages, copy the FCC pages and the **`js`** directory available at the following location to an appropriate location on the Web Server where the SiteMinder Web Agent is installed.

`<installation_dir>/adapterSiteMinder/fcc/`

In addition to copying the files, you must also create a virtual directory on the Web Server that points to the directory where the `js` directory and FCC pages are copied.

By default, Arcot uses **`arcotlogin`** as the name of the virtual directory. If you use a different name, then you must edit the *<path>* of the following parameters found in the **`adaptershim.ini`** file:

- ErrorPageURL
- InitialFCCURL
- FinalFCCURL

Deploying Authentication Shim

The files required to deploy the Authentication Shim are available at the following location:
`<installation_dir>/adapterSiteMinder/lib/`

To deploy the Authentication Shim:

- The SiteMinder Policy Server requires the Authentication Shim library and the log library files to be present in the `LD_LIBRARY_PATH` variable. You can do this by:

Note: If you perform the following operations when the SiteMinder Policy Server is running, then you must restart the SiteMinder Policy Server.

  - Copying the `libArcotSiteMinderAdapter.so` and `ArcotLog2FileSC.so` files, available at:

    `<installation_dir>/adapterSiteMinder/lib`

    to the `lib` directory of the SiteMinder Policy Server.

    or

  - Including the `<installation_dir>/adapterSiteMinder/lib` directory in `LD_LIBRARY_PATH`.

Enabling SSL

It is recommended that you enable the Authentication Shim for SSL communication. To enable the Authentication Shim to communicate with State Manager over SSL, you must set the following configuration parameters in **`adaptershim.ini`** file:

- ArcotSMTrustedRootPEM
- ArcotSMClientSSLCert
- ArcotSMClientPrivateKey

Configuring Shim

The Authentication Shim configurations are performed in the `adaptershim.ini` file. This file defines the configuration parameters that must be set for Arcot Adapter and CA SiteMinder WAM to communicate with each other. The file is installed at the following location:

`<installation_dir>/conf`

The section `[arcot/integrations/smadapter/Default]`, contains the parameters that you need to set according to the authentication flow that you want to use. Table 6-1 explains the parameters of this section.

Table 6-1. Configuration Parameters

Parameter	Required/ Optional	Description
`DisambigSchemeLib`	Optional	Specify the DLL library name of an authentication scheme to use for user disambiguation. **Note:** This parameter does not support refresh option, which means if you switch to use Adapter authentication, then you must restart the SiteMinder Policy Server.
`DisambigSchemeParam`	Optional	Specify the parameter string to pass to the disambiguation authentication scheme. This must be structured the same way as the SiteMinder Policy Server would build the string from the configuration parameters for the scheme.
`AuthSchemeLib`	Optional	Specify the library name of an authentication scheme to use as a backing scheme for primary authentication. **Note:** This parameter does not support refresh option, which means if you switch to use Adapter authentication, then you must restart the SiteMinder Policy Server. **Note:** This parameter is not used for delegated authentication scenario.

Table 6-1. Configuration Parameters

Parameter	Required/ Optional	Description
`AuthSchemeParam`	Optional	If the backing authentication scheme is configured, this parameter is passed to it as its configuration string. It must be set to have the same content, as the SiteMinder Policy Server would set from the scheme configuration dialog. You can determine this by examining the scheme setup dialogs in the SiteMinder Policy Server administration interface. As you change parameters, the dialog shows the **Parameter** that the SiteMinder Policy Server would send. **Note:** This parameter is not used for delegated authentication scenario.
`ArcotSMBaseURL`	Required	Specify the URL where the State Manager is available. The syntax to specify the State Manager's URL is: *https://<Host>:<Port>/arcotsm/servlet/*
`ArcotSMRetries`	Required	Specify the maximum number of retries allowed to connect to the State Manager. If this value is `0`, it signifies only one connection attempt is allowed. Default value: **`0`**
`ArcotSMResponseWait`	Required	Specify the time period (in seconds) for which the Shim will wait for the State Manager to respond before logging an error. Default value: **`30`**
`ArcotSMTrustedRootPEM`	Required, *If* HTTPS is enabled	Provide the location of the certificate of the trusted root certificate authority, if the State Manager is enabled for HTTPS. The file *must* be in `.PEM` format.
`ArcotSMClientSSLCert`	Required, *If* HTTPS is enabled	Provide the location of the client-side SSL certificate, if the State Manager is enabled for HTTPS. The file *must* be in `.PEM` format.
`ArcotSMClientPrivateKey`	Required, *If* HTTPS is enabled	Provide the private key of the client in `.PEM` format, if the State Manager is enabled for HTTPS. The file *must* be in `.PEM` format.

Table 6-1. Configuration Parameters

Parameter	Required/ Optional	Description
`ArcotAFMLandingURL`	Required	The controller JSP URL of the AFM. **Note:** Although you can use multiple sample flows, but only one `ArcotAFMLandingURL` can be configured per section.
`UseCustomizationEngineAuth`	Optional	Specify whether to use AFM to perform authentication: • OnePage - `false` • TwoPage - `false` • DelegatedAuth - `true` • UseHTMLAuth - `false` Default value: **`false`**
`InitialPhasePrimaryAuth`	Optional	Specify whether to perform LDAP authentication before risk evaluation or after. This parameter is applicable if `UseCustomizationEngineAuth` is set to `false`. Default value: **`true`** *(LDAP authentication is performed before risk evaluation)*
`ErrorPageURL`	Required	Specify the URL of the error FCC page. This page will be displayed to the user in case of any error.
`InitialFCCURL`	Required	Specify the URL of the initial FCC page served to the user. The Shim reports this URL to CA SiteMinder WAM during initialization. When the user attempts to access a protected resource and authentication is required, CA SiteMinder WAM directs the user to this page. Depending on the authentication flow, the page can collect information such as, the username, or username and password.
`FinalFCCURL`	Required	Specify the URL that is used by the AFM to forward the control back to the Shim. The AFM retrieves this URL from the token.

Configuring Global Information

The global Authentication Shim configuration parameters are available in the `GLOBAL SETUP` section of the `adaptershim.ini` file. The following table describes the parameters of `[arcot/integrations/smadapter]` section.

Table 6-2. Global Configuration Parameters

Parameter	Required/ Optional	Description
`WatchInterval`	Required	Specify the polling interval (in seconds) for the Authentication Shim to use for monitoring the configuration file. The Authentication Shim allows configuration changes without re-starting the SiteMinder Policy Server. It monitors the configuration file at this interval and if the file has changed, it reloads the configurations. Default value: **`300`**
`ShimIdentifierString`	Optional	Specify a unique identifier of the Authentication Shim instance. The value that you specify is appended with section name to create identifier.
`LogSupported`	Required	Specify whether to enable logging for the Authentication Shim. Set this to **`1`** if you want enable logging, or set this value to **`0`** for no logging.
`MultipleUserDirectoriesSupported`	Optional	Specify whether to enable multiple user directory support. If it is set to `1`, then the multiple directory support would be enabled. Default value: **`0`** *(disabled)*
`SmApiVersion`	Optional	Specify the supported version of the SiteMinder API. Supported Values: • `300` • `400` • `401` Default value: **`400`**

Configuring the Log Information

The Authentication Shim generates log messages as a part of its operation to support error reporting, auditing, and debugging. The level of details logged by the Authentication Shim can be configured.

All Authentication Shim log messages, except trace messages, are written to the SiteMinder Policy Server log file (`smps.log`). All trace messages are logged in the files that are configured in the SiteMinder Policy Server.

All entries that are logged in the `smps.log` file are also logged in the Adapter log file (`arcotadaptershim.log`). However, the level of message details in the Adapter log file is determined by the `HandleLevel` parameter.

The log-related parameters are in the `LOGGING SETUP` section of the `adaptershim.ini` file. The log-related topics are described in the following subsection.

Setting up Log Parameters

The following table describes the log parameters defined in the `[arcot/integrations/smadapter/LogLibrary<n>]` section.

Table 6-3. Log Configuration Parameters

Parameter	Required/ Optional	Description
`DLLName`	Optional	Set the parameter `DLLName` to the name of the library file that performs the logging. **Note:** *Do not* specify the suffix of the file name, because it is automatically added during the run-time. Default value: **`ArcotLog2FileSC`**
`HandleLevel`	Optional	Specify the log level, which defines the details that must be included in the log messages. Severity message of the specified level and the higher level are logged. For example, if the value is set to 2, then the messages of severity level 2 to 7 are logged. Supported Values: • `1=low` • `2=info` • `3=notice` • `4=warning` • `5=error` • `6=alert` • `7=fatal` Default value: **3**

Table 6-3. Log Configuration Parameters

Parameter	Required/ Optional	Description
`EntryPoint`	Optional	Specify the function within the library that must be called to get a handle to the logging object. **Note:** This is fixed for a given log handler DLL. Default value: **`CreateFileLogHandler`**
`ParamSupported`	Optional	Specify the count of parameters to pass to the logging object. Default value: **`4`**
`Param1=LOG_FILE_NAME`	Optional	Specify the name and location of the log file. Default value: ***`<installation_dir>`*`/logs/arcotadaptershim.log`**
`Param2=LOG_FILE_ROLLOVER_INTERVAL`	Optional	Specify how often you want to rollover the log file to a backup file. Supported Values: • `HOURLY` • `DAILY` • `WEEKLY` • `MONTHLY` Default value: **`DAILY`**
`Param3=MAX_LOG_FILE_SIZE`	Optional	Specify the maximum size of the log file. This is an alternative way to indicate rollover, if the rollover interval is not set. The size is expressed in bytes. For example: `Param3=MAX_LOG_FILE_SIZE=10000000` The above value indicates the size of the log file is approximately`10` MB. **Note:** If this parameter is set to `0`, the log file will continue to grow indefinitely.
`Param4=BACKUP_LOG_FILE_LOCATION`	Optional	Specify the complete path where the backup log file will be stored. The path provided must be valid. Default value: ***`<installation_dir>`*`/logs/backup`**

Table 6-3. Log Configuration Parameters

Parameter	Required/ Optional	Description
`Param5=LOG_LINE_ FORMAT`	Optional	Specify the format of the logging string. This indicates the attributes that will be logged on each line of the file. **Note:** If this parameter is not set, the legacy format will be used. Supported Values: • `LTZ`=System Timezone, Date, and Time • `SEV`=Severity • `PID`=ProcessID • `TID`=ThreadID • `MID`=MessageIDNumber • `MSG`=Log Message Text • `LID`=LoggingID

Testing the Configuration

To test the Authentication Shim configuration:

1. Open the `arcotadaptershim.log` log file available in the following directory:

Note: By default, the installer does not create this file. It is generated when the Authentication Shim receives the first authentication request.

`<installation_dir>/logs`

2. Search for the following entry in the log file, which indicates the Authentication Shim is configured successfully.

```
Logger initialized
STARTING [Arcot Adapter 2.2]
Starting watchdog thread...
```

Chapter 7
Configuring CA SiteMinder Policy Server

This chapter lists the CA SiteMinder Policy Server configurations that you must perform after completing the installation and configuration of the Adapter components.

Perform the following steps to configure SiteMinder Policy Server to use Arcot Adapter:

1. To configure the Arcot Adapter, you must create a custom Authentication Scheme in CA SiteMinder WAM. In the SiteMinder Policy Server administration tool, create a new Authentication Scheme as follows:
   a. In the SiteMinder Authentication Scheme Dialog screen, enter the name for the Authentication Scheme and provide the description for the same.
   b. Select the **Authentication Scheme Type** as **Custom Template**.
   c. Enter the Adapter library file name (`ArcotSiteMinderAdapter`) in the **Library** field.
   d. Enter the name of the configured flow in the **Parameter** field, this must correspond to section name in the `adaptershim.ini` file. Following are the default values that are provided in the `adaptershim.ini` file:
      - `OnePage`
      - `TwoPage`
      - `DelegatedAuth`
      - `UseHTMLAuth`

Note: On UNIX platforms, you must append the section name with the `<installation_dir>` separated by a comma, for example `[SectionName],[installation_dir]`. There should not be any whitespace character between the section names and comma. For example, if your section name is OnePage, then the parameter must be specified as `OnePage,/opt/arcot`.

2. For any realm that you wish to protect with Arcot authentication, it must be configured to use the new Authentication Scheme that you created in Step 1. Use **SiteMinder Realm Dialog** to perform this operation.

3. For SiteMinder Policy Server to work with Arcot Adapter, set the following parameters in the **SiteMinder Agent Configuration Object Dialog**:
   - **CssChecking** - Set this to YES.
   - **FCCCompatMode** - Set this to YES.
   - **AgentName** - Set this to the name of the agent.
   - **LogFileName** - Enter the log file name of the Web Agent. (This is not a mandatory setting, but can be used for debugging.)
   - **DefaultAgentName** - Enter the name of the default Web Agent.
   - **DefaultPassword** - Enter the Web Agent password.
   - **LogFileSize** - Enter the size of the Web Agent log file.
   - **LogFile** - Set this to YES.
   - **RequireCookies** - Set this to YES.
   - **TraceConfigFile** - Enter the name of the trace configuration file. (This is not a mandatory setting, but can be used for debugging.)
   - **TraceFile** - Set this to YES.
   - **TraceFileName** - Enter the name of the trace file.
   - **TraceFileSize** - Enter the size of the trace file.

Chapter 8
Uninstalling Arcot Adapter Components

Before you uninstall Arcot Adapter, you should first remove its database schema and then proceed with the uninstallation process. After you complete the uninstallation, you must then perform the post-uninstallation tasks to clean up the residual WAR files.

This chapter guides you through the steps for uninstalling Arcot Adapter and its components. The chapter covers the following sections:

Dropping Adapter Schema

Note: If for some reason, you need to retain the database, then *do not* proceed with the instructions in this section. Refer to section "Uninstalling Arcot Adapter" to proceed with the uninstallation.

Perform the following tasks to uninstall the Adapter database schema:

1. Navigate to the following directory:

```
<installation_dir>/dbscripts/oracle/
```

2. If you are using a single database for all Arcot products, then execute the following command in your database:

```
DROP TABLE ARTSTOKENS;
```

or

If you are using a separate database for Arcot Adapter, then either execute **drop-adapter-statemanager-2.2.sql** file or execute the following commands in your database:

```
DROP TABLE ARTSTOKENS;
DROP TABLE ARCMNDBERRORCODES;
```

This drops all database tables created by Adapter.

Uninstalling Arcot Adapter

To uninstall Arcot Adapter, you need to remove the components installed during the installation process. Perform the following steps to uninstall Arcot Adapter:

1. Navigate to the following directory:

   `<installation_dir>/Uninstall_Arcot Adapter 2.2/`

Note: If the Arcot Adapter installer has been configured to run in the *Silent Mode*, then you need to execute the following command to start the uninstallation process:

`prompt>./Uninstall_Arcot_Adapter_2.2 -i silent`

The uninstallation processes would not display any interactive dialogs while running. After executing the above-mentioned command, proceed with the "Post-Uninstallation Steps".

2. Run the installer using the following command:

   `prompt>./Uninstall_Arcot_Adapter_2.2`

   The Uninstall Options screen appears.

3. Select the type of uninstallation:

   - **1-Completely remove all components... :** Select this option if you want to uninstall *all* components of the Arcot Adapter from the current system.
   - **2-Choose specific components... :** Select this option if you want to uninstall only *selected* components of the Arcot Adapter from the current system.

4. Press **Enter** to continue.

If you selected to uninstall all components, proceed to Step 7.

If you selected to uninstall selected components, the Choose Product Components screen appears.

5. (*For Uninstalling Specific Components Only*) This screen displays the Arcot Adapter components that are installed on the current system. By default, all installed components are selected for uninstallation. Enter the number of the components (separated by a comma) that you *do not* want to uninstall from the current system.
6. Press **Enter**.

   The Choose Backup Location screen appears.
7. If you want to take a backup of important files such as the configuration or log files, specify a location where you want to store these files and press **Enter** to uninstall Arcot Adapter components.

   The Uninstall Complete screen appears at the end of successful uninstallation and the system returns to the command prompt.

Post-Uninstallation Steps

Perform the following post-uninstallation steps:

1. Delete the installation directory (`<installation_dir>`).

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

2. If you have installed State Manager and Authentication Flow Manager, then uninstall the following `WAR` files from the appropriate location on your application server.
   - `arcotafm.war` - Authentication Flow Manager
   - `arcotsm.war` - State Manager

For example, on Apache Tomcat the location is `<application_server_home>/webapps`. Here, *`application_server_home`* represents the directory path, where Apache Tomcat is installed.

Note: If you have performed distributed-system deployment, then locate and uninstall these `WAR` files from the system where you have deployed the particular component.

Appendix A
Configuring Backing Authentication Scheme

This release of Adapter supports external or third-party authentication schemes or mechanisms. These mechanisms are referred to as *backing authentication* in the Adapter terminology.

If a backing authentication scheme is configured, the Arcot Authentication Shim acts as an interface between CA SiteMinder and the backing authentication mechanism. It forwards the authentication requests to the backing method, and when it receives the authentication result back from the backing authentication method, it posts the same to CA SiteMinder Policy Server. In this case, the Adapter can just be used for risk evaluation.

When a backing authentication scheme is configured for the Arcot Authentication Shim, it dynamically loads the external authentication scheme. The Authentication Shim can also delegate the CA SiteMinder authentication calls to the backing authentication scheme.

Typically, Authentication Shim is transparent to the backing authentication scheme. However, if the Authentication Flow Manager directs that the transaction should be terminated immediately (for example, risk evaluation indicates `DENY`), then the Authentication Shim can override successful authentication result from the backing authentication scheme.

This appendix walks you through the process of configuring a backing authentication scheme with the Adapter:

1. Configuring Shim for Backing Authentication Scheme
2. Configuring Policy Server for Backing Authentication Scheme
3. Configuring FCC Pages

Configuring Shim for Backing Authentication Scheme

The authentication scheme is configured by using the CA SiteMinder Policy Server administration interface. Backing authentication schemes, however, are loaded by the Arcot Authentication Shim and not by the Policy Server. Therefore, most of their configuration is specified in the Authentication Shim configuration file.

The following three parameters must be configured in `adaptershim.ini` to use a backing authentication scheme:

1. Scheme DLL Name (**`AuthSchemeLib`**)

   The shared library name for the backing authentication scheme is configured in the Authentication Shim configuration file, as `AuthSchemeLib` parameter for authentication.

2. Scheme Parameter String (**`AuthSchemeParam`**)

   Most scheme configuration data is stored in the parameter string. This string is configured by using the `AuthSchemeParam` in the Authentication Shim configuration file. The content of this string is specific to the backing authentication scheme you are using.

3. FCC URLs (**`ErrorPageURL`** and **`FinalFCCURL`**)

   The Adapter serves these FCC pages to the user for handling user interactions and for handling errors. Ensure that these are configured to point to:

   - `ErrorPageURL: shimerror.fcc`
   - `FinalFCCURL: shimfinal.fcc`

Configuring Policy Server for Backing Authentication Scheme

If the scheme requires a shared secret, then it must be configured in the Policy Server administration interface as the **Shared Secret** for the Arcot Authentication Shim scheme. The Authentication Shim, which itself does not use a shared secret, passes this parameter to the backing authentication scheme.

Note: If backing authentication schemes are used for disambiguation and authentication, then they must use the same shared secret, because *only one* shared secret can be configured.

The Policy Server administration interface can help you determine the library name and the proper configuration string for a given scheme. Using it, you can create a sample scheme configuration. The interface enables you to set the various scheme parameters and shows you the resulting string.

In CA SiteMinder Policy Server version 12, create an authentication scheme with the appropriate template. The **Scheme Setup** section of the creation page shows the **Library** and **Parameter** fields.

Book: Refer to the CA documentation for more information.

Configuring FCC Pages

To configure the FCC pages to accommodate the backing authentication scheme:

1. Include **`ArcotAdapterIntegration.js`** in your code:

```
<script type="text/javascript"
src="js/ArcotAdapterIntegration.js"></script>
```

2. Include the following in your HTML code *before* processing anything related to `smusermsg`:

```
<div id="formDiv" style="display:none">
            <form name=authUsrMsgForm>
             <textarea name=authUsrMsgTxtArea COLS=0
ROWS=0>$$smusrmsg$$</textarea>
            </form>
</div>
```

3. Extract the value of the **`smUserMsg`** variable by using the **`ArcotExtractUserMsg()`** function:

```
smUserMsg =
ArcotExtractUserMsg(document.authUsrMsgForm.authUsrMsgTxtArea.value)
;
```

4. Before submitting the form, call the **`ArcotPrepareSubmit()`** function:

```
ArcotPrepareSubmit(document.Login,
document.authUsrMsgForm.authUsrMsgTxtArea.value);
document.Login.submit();
```

Sample FCC Code

The following is a sample FCC code that illustrates the FCC modifications required for implementing your backing authentication scheme.

```
------------------------------------------------------------------
@username=%USER%
@smretries=0


<!-- SiteMinder Encoding=ISO-8859-1; -->
<html>
<head>
<title>Any Authentication Scheme for SiteMinder</title>
<meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">


<script type="text/javascript"
src="js/ArcotAdapterIntegration.js"></script>



<script language="javascript" type="text/javascript">


var smUserMsg;
function login() {
         // Process form for submission.
         // ....
         // ....
         // ....
```

```
        // Previously
        // document.Login.submit();

        // Change to
        ArcotPrepareSubmit(document.Login,
document.authUsrMsgForm.authUsrMsgTxtArea.value);
        document.Login.submit();
}


function ProcessSMUserMsg() {
        // previously
        // smUserMsg = $$smusrmsg$$;

        // change to
        smUserMsg =
ArcotExtractUserMsg(document.authUsrMsgForm.authUsrMsgTxtArea.value);



        // Use the variable smUserMsg like before
        // .....
        // .....
        // .....

}


</script>
</head>
```

```
<body>
<h3>Any Authentication Scheme for SiteMinder</h3>

<!--
Arcot Form to get siteminder user msg.
have this always before processing anything related to smusermsg.
-->
<div id="formDiv" style="display:none">
            <form name=authUsrMsgForm>
             <textarea name=authUsrMsgTxtArea COLS=0
ROWS=0>$$smusrmsg$$</textarea>
            </form>
</div>



<script>
ProcessSMUserMsg();
</script>

<form NAME="Login" METHOD="POST">
      <INPUT TYPE="HIDDEN" NAME="SMENC" VALUE="ISO-8859-1">
      <INPUT type="HIDDEN" name="SMLOCALE" value="US-EN">
      <input type="password" name="PIN" size="11" style="margin-left:
1px">
      <input type="hidden" name="target" value="$$target$$">
      <input type="hidden" name="smauthreason"
value="$$smauthreason$$">
      <input type="hidden" name="smagentname" value="$$smagentname$$">
      <input type="hidden" name="type" value="$$type$$">
      <input type="hidden" name="realmoid" value="$$realmoid$$">
      <input type="hidden" name="USER" value="">
      <input type="hidden" name="PASSWORD" value="">
```

```
      <input type="button" value="Login" onClick="login();">
</form>

</body>
</html>
-----------------------------------------------------------------
```

Appendix B
New File and Property Names

This appendix lists the files and properties that have been renamed in the current release of Arcot Adapter 2.2. This appendix contains the following sections:

Updated File Names

The following table lists the components affected by the file name change, and the files that have been renamed in the current release of Arcot Adapter.

Table B-1. Updated File Names

Component	Old File Name in Adapter 2.1 or Earlier	New File Name in Adapter 2.2 or Later
Authentication Flow Manager (formerly known as *Arcot Customization Engine*)	`arcotauthui.war`	`arcotafm.war`
	`arcotauthui.properties.src`	`arcotafm.properties.src`
	`arcotauthui.properties`	`arcotafm.properties`
State Manager (formerly known as *Token Server*)	`arcottoksvr.war`	`arcotsm.war`
	`arcottokenserver.properties.src`	`arcotsm.properties.src`
	`arcottokenserver.properties`	`arcotsm.properties`

Updated Property Names

The following table lists the property names that have changed in the current release of Arcot Adapter along with the components affected by this change.

Table B-2. Updated Property Names

Component	Old Property Name in Adapter 2.1 or Earlier	New Property Name in Adapter 2.2 or Later
Authentication Flow Manager (formerly known as *Arcot Customization Engine*)	ArcotAuthUILandingURL	ArcotAFMLandingURL
	TokenServerHostname	ArcotSMHostname
	TokenServerPort	ArcotSMPort
	TokenServerURLBase	ArcotSMBaseURL
	TokenServerSecureConnection	ArcotSMSecureConnection
	TokenServerTrustStore	ArcotSMTrustStore
	TokenServerTSPassword	ArcotSMTrustStorePassword
	TokenServerKeyStore	ArcotSMKeyStore
	TokenServerKSPassword	ArcotSMKeyStorePassword
	TokenServerConnTimeoutMS	ArcotSMConnTimeoutMS
	TokenServerReadTimeoutMS	ArcotSMReadTimeoutMS
	TokenServerTestConnAtStartup	ArcotSMTestConnAtStartup
	WebFortHostname	WebFortremotehost.1
	WebFortPort	WebFortremoteport.1
	WebFortTransport	WebFortransport
	WebFortCA_CERT_FILE	WebFortserver.CACert
	WebFortMaxConnPoolSize	WebFortpool.maxactive
Authentication Shim (formerly known as *Shim for CA SiteMinder)*	TokenServerBaseURL	ArcotSMBaseURL
	TokenServerRetries	ArcotSMRetries
	TokenServerResponseWait	ArcotSMResponseWait
	TokenServerTrustedRootPEM	ArcotSMTrustedRootPEM
	TokenServerClientSSLCert	ArcotSMClientSSLCert
	TokenServerClientPrivateKey	ArcotSMClientPrivateKey

Appendix C
Third-Party Software Licenses

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

Apache

- Copyright © 2009 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.
  - `annogen-0.1.0.jar`
  - `axiom-api-1.2.7.jar`
  - `axiom-dom-1.2.7.jar`
  - `axiom-impl-1.2.7.jar`
  - `axis2-adb-1.4.1.jar`
  - `axis2-adb-codegen-1.4.1.jar`
  - `axis2-ant-plugin-1.4.1.jar`
  - `axis2-clustering-1.4.1.jar`
  - `axis2-codegen-1.4.1.jar`
  - `axis2-corba-1.4.1.jar`
  - `axis2-fastinfoset-1.4.1.jar`
  - `axis2-java2wsdl-1.4.1.jar`
  - `axis2-jaxbri-1.4.1.jar`
  - `axis2-jaxws-1.4.1.jar`
  - `axis2-jaxws-api-1.4.1.jar`
  - `axis2-jibx-1.4.1.jar`
  - `axis2-json-1.4.1.jar`
  - `axis2-jws-api-1.4.1.jar`
  - `axis2-kernel-1.4.1.jar`
  - `axis2-metadata-1.4.1.jar`
  - `axis2-mtompolicy-1.4.1.jar`
  - `axis2-saaj-1.4.1.jar`

- axis2-saaj-api-1.4.1.jar
- axis2-spring-1.4.1.jar
- axis2-xmlbeans-1.4.1.jar
- commons-fileupload-1.2.jar
- commons-io-1.4.jar
- commons-logging-1.1.1.jar
- geronimo-annotation_1.0_spec-1.1.jar
- geronimo-stax-api_1.0_spec-1.0.1.jar
- httpcore-4.0-beta1.jar
- httpcore-nio-4.0-beta1.jar
- jettison-1.0-RC2.jar
- log4j-1.2.15.jar
- woden-api-1.0M8.jar
- woden-impl-dom-1.0M8.jar
- wstx-asl-3.2.4.jar
- xalan-2.7.0.jar
- xercesImpl-2.8.1.jar
- xml-apis-1.3.04.jar
- xml-resolver-1.2.jar
- xmlbeans-2.3.0.jar
- XmlSchema-1.4.2.jar
- neethi-2.0.4.jar
- soapmonitor-1.4.1.jar
- mex-1.4.1.jar
- commons-codec-1.3.jar
- commons-collections-3.1.jar
- commons-httpclient-3.1.jar
- commons-lang-2.4.jar
- commons-pool-1.4.jar
- ibatis-2.3.4.726.jar
- opensaml-2.2.3.jar

- `openws-1.2.2.jar`
- `joda-time-1.5.2.jar`
- `velocity-1.5.jar`
- `xmlsec-1.4.2.jar`
- `xmltooling-1.2.0.jar`

- The Apache Software License, Version 1.1. Copyright© 2000 The Apache Software Foundation. All rights reserved.
  - `log4j-1.2.9.jar`

Common Development and Distribution License (CDDL) version 1.0

- `activation-1.1.jar`
- `mail-1.4.jar`
- `jaxb-api-2.1.jar`
- `jaxb-impl-2.1.6.jar`
- `jaxb-xjc-2.1.6.jar`
- `json-lib-0.7.1.jar`

Copyright © 2003-2007, Dennis M. Sosnoski. All Rights Reserved.

- `jibx-bind-1.1.5.jar`
- `jibx-run-1.1.5.jar`

Creative Commons Public Domain

- `backport-util-concurrent-3.1.jar`

jalopy-1.5rc3.jar

Copyright © 2001-2004, Marco Hunsicker. All rights reserved.

jaxen-1.1.1.jar

Copyright 2003-2006 The Werken Company. All Rights Reserved.

Json2.js

Copyright© 2002 JSON.org

json-lib-0.7.1.jar

Copyright© 2002 JSON.org

Oracle Database 10*g* JDBC Driver

QOS.ch Copyright © 2004-2008

- `slf4j-api-1.5.5.jar`
- `slf4j-simple-1.5.2.jar`

SWFObject

wsdl4j-1.6.2.jar

Common Public License - v 1.0

Other Trademarks

- UNIX® is a registered trademark of The Open Group in the United States and other countries.
- Linux® is a trademark of Linus Torvalds in the U.S., other countries, or both.
- Java™ and all Java-based trademarks are trademarks of Oracle® in the United States, other countries, or both. Other company, product, and service names may be trademarks or service marks of others.
- BEA WebLogic Server® and Solaris SPARC are trademarks of Oracle® in the United States and other countries.

Appendix D
Glossary

ArcotID	Is a secure software credential that supports two-factor authentication. To authenticate to WebFort using ArcotID, the user needs the ArcotID file and the associated password.
Arcot Adapter	Arcot product that increases the security of Web applications and protects resources by providing software-based strong authentication system.
Delegated Authentication	In this method the authentication and risk processing is done by Arcot WebFort and Arcot RiskFort respectively. The Arcot Authentication Shim redirects the user to Authentication Flow Manager, which does the authentication and risk processing and then returns the control back to CA SiteMinder WAM. There are two scenarios in this type: 1. Only ArcotID authentication 2. ArcotID authentication and risk evaluation
Authentication Flow Manager	A component of Arcot Adapter that interacts with Arcot WebFort (and Arcot RiskFort, if configured) and takes the end user through the configured authenticate flow. Authentication Flow Manager is a set of JavaServer Pages (JSPs).
One-Page Login	It is an authentication flow, in which the user enters the user name and password in `shim.fcc` page. After successful user authentication and risk evaluation, the user is provided access to the protected page.
Personal Authentication Message	A secret message set up by the user when the user is enrolled or when the account is created. It is presented to the user (usually after risk evaluation) to assure the user that the user is interacting with the correct and legitimate server. This is also referred to as "server authentication," because it authenticates the server to the user.
Primary authentication	The authentication mechanism used for the primary or main authentication of users. If only one authentication mechanism is used, then it is the primary authentication mechanism.
Question and Answer	Type of authentication method supported by WebFort. In this method, the user sets questions and answers during enrollment. The user has to answer these security questions during authentication.

RiskFort	RiskFort provides a mechanism to evaluate the risk of a given transaction.
Risk Advice	An action (`ALLOW`, `ALERT`, `DENY`, `INCREASEAUTH`) suggested by RiskFort to the calling application, after evaluating the risk of a transaction.
Risk Score	RiskFort generates a score depending on the evaluation result. The score can be a number from 0 through 100. The greater the number, the higher the risk.
Roaming Download	The process of downloading ArcotID, on a system other than the primary system, from the WebFort Server.
Secondary Authentication	This is a step-up authentication, which the user has to perform in any of the following cases: • If the risk advice is `INCREASEAUTH` • If the user is downloading ArcotID from WebFort **Note:** QnA method is used as a secondary authentication method. You can use any customized authentication methods for this purpose.
CA SiteMinder Authentication Shim	Component of Arcot Adapter that redirects the user to other components for authentication and risk evaluation.
State Manager	Component of Arcot Adapter that generates the token for the user to keep track of the user information.
Two-Page Login	It is an authentication flow, in which the user enters the user name first and after the secondary authentication the user enters the password. If authenticated successfully, the user is granted access to the protected resource The `shim2.fcc` page is used in this authentication flow.
WebFort	WebFort provides two-factor software-based strong authentication.