CA Adapter

Installation and Configuration Guide for UNIX

r2.2.9

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction to Adapter 9

Adapter Integration Options 11
- Adapter for SAML 11
- Adapter for SiteMinder 11
- Adapter for VPN 12

Adapter Architecture 12
- Authentication Flow Manager 14
- State Manager 17
- User Data Service 17
- Authentication Shim 18
- Form Credential Collector (FCC) Pages 18
- VPN Client 18
- Other Authentication Products Used with Adapter 18

Adapter Workflows 19
- End User Login Workflow in SAML 20
- End User Authentication Workflow in SiteMinder 21
- End User Authentication Workflow in IPSec VPN 21
- End User Authentication Workflow in SSL VPN 22

Adapter Features 22

Chapter 2: Planning the Deployment 23

Deployment Architecture 23

Deployment Overview 25

Chapter 3: Preparing for Installation 29

Software Requirements for State Manager 29
- Minimum Software Requirements 29
- Configuring the Application Server 31

Software Requirements for Authentication Flow Manager 31

Software Requirements for Authentication Shim 33

Software Requirements for FCC Pages 33

Checklist for Integration 34

Chapter 4: Installing Adapter 37

Installing in a Distributed Environment 37

For SiteMinder Integration....38
For SAML Integration....41
For VPN Integration....43
Installing on a Single System....44
Verifying the Installation....45

Chapter 5: Performing Adapter Configuration Using the Wizard 47

Understanding the AFM Profile....48
Deploying the Wizard....49
Configuring Adapter by Using the Wizard....50
Copying the Adapter Configuration Files....64
For SiteMinder Integration....65
For SAML Integration....65
For VPN Integration....65

Chapter 6: Deploying and Configuring State Manager 67

Running Database Scripts....67
Copying the JDBC Drivers....68
Apache Tomcat....69
JBoss....69
(For Microsoft SQL Server) Oracle WebLogic....70
Creating a JNDI Connection....70
Apache Tomcat (C7_CJNDI_TOMCAT)....71
IBM WebSphere....73
JBoss....76
Oracle WebLogic....77
Deploying State Manager....78

Chapter 7: Deploying and Configuring Authentication Flow Manager 81

Deploying Authentication Flow Manager....82
Next Steps....86

Chapter 8: Configuring Authentication Shim and FCC Pages 87

Deploying the FCC Pages....87
Deploying Authentication Shim....87

Chapter 9: Configuring CA SiteMinder Policy Server 89

Chapter 10: Deploying and Configuring SAML Sample Applications 93

Chapter 11: Deploying the Sample Application WAR Files 93

Chapter 12: Verifying the Sample Application Deployment 97

Chapter 13: Configuring Sample Application 97

Chapter 14: Performing Basic AFM Configurations Using Sample Application 97

Chapter 15: (Optional) Configuring Custom Certificates in Sample Application 98

Chapter 16: Configuring the Service Provider's Application 101

Chapter 17: Verifying Adapter Integration 103

Verifying the State Manager Configuration 103
Verifying the AFM Configuration 104
Verifying the Authentication Shim Configuration 104
Verifying SiteMinder Integration 105
Verifying SAML Integration 105

Chapter 18: Uninstalling Adapter 107

Dropping the Adapter Schema 107
Uninstalling Adapter 108
Post-Uninstallation Steps 109

Appendix A: Adapter File System Structure 111

Appendix B: Configuration Files and Options 119

State Manager Properties File 119
State Manager Log File 123
AFM Properties File 124
AFM Log File 146

SAML Properties File 146
Authentication Shim Properties File 150
Configuring Global Information 153
Configuring the Log Information 154

Appendix C: Deploying and Configuring the Custom Application 159

Custom Application Deployment Architecture 159
Deploying the Custom Application WAR Files 160
Verifying the Custom Application Deployment 161
Configuring the Custom Application 162
Testing the Custom Application 163

Appendix D: Additional Configurations to Support LDAP Repository in AuthMinder 165

Creating Organization in LDAP Repository 166
Resolving Credential Types for LDAP Organization 171
Verifying the LDAP Configuration in AuthMinder 171

Appendix E: Configuring SSL in Apache Tomcat 173

Configuring SSL 174
Verifying the SSL Configuration in Tomcat 175

Chapter 1: Introduction to Adapter

Organizations use various authentication methods to secure access to the resources available in their private networks. Basic authentication methods, such as user name and password, while protecting the integrity of data transmissions, expose organizations to the risk of identity fraud. Authentication methods that utilize hardware devices, such as *One-Time Password* (OTP) tokens, are expensive to deploy and manage. Also, the problem of Identity Management is compounded by the increasing number of applications in a network. Each application requires a unique username and password to be remembered by the end user, and applications need dedicated resources to store and manage the user credentials. Therefore, the need for *Single Sign-On* (SSO) and multi-factor authentication services is pivotal for organizations to provide secure access to protected resources.

Adapter provides SSO and multi-factor authentication services for multiple Web applications. It enables organizations to upgrade from the standard user name and password authentication mechanism, without changing their users login experience or their critical business processes.

Adapter combines a flexible, software-based strong authentication solution, and a risk-based adaptive authentication solution to provide a robust and secure solution for accessing Web applications, such as:

- SAML-based Web portals
- Web Access Management solutions, such as SiteMinder
- *Internet Protocol Security* (IPSec) or SSL-based *Virtual Private Network* (VPN) appliances

This guide provides information for installing and configuring Adapter on supported UNIX platforms with supported applications, such as CA SiteMinder, *Security Assertion Markup Language* (SAML) based Web portals, or *Virtual Private Network* (VPN) applications. This guide describes the following:

- The high-level architecture of the integration process
- Components of Adapter
- Requirements for installing Adapter
- Installing and configuring Adapter to work with the supported applications
- Uninstalling Adapter

This chapter introduces you to the basic concepts of Adapter and covers the following topics:

- Adapter Integration Options (see page 11)
- Adapter Architecture (see page 12)
- Adapter Workflows (see page 19)
- Adapter Features (see page 22)

Note: CA Adapter still contains the terms Arcot, WebFort and RiskFort in some of its code objects and other artifacts. Therefore, you will find occurrences of Arcot, WebFort and RiskFort in all CA Adapter documentation. In addition, some of the topics in this guide do not follow the standard formatting guidelines. These inconsistencies will be fixed in a future release.

Adapter Integration Options

Adapter can integrate with the following types of applications:

- SAML-based Web portals
- SiteMinder
- IPSec or SSL-based VPNs

The following subsections describe these integration options.

Adapter for SAML

By integrating Adapter with your business applications and resources, you enable a solution that provides secure Single Sign-On access for all your Web applications using Security Assertion Markup Language (SAMLv2). As a result, users can log in once and gain access to all applications without having to individually log in to each of them.

When users are enrolled in Adapter, they are provided an AuthMinder credential that is subsequently used as the authentication credential in one or more applications. As you add subsequent applications and "link" them, you can use the same credential that you set up for the first application. Any time you change your password or other authentication credentials within one application, it will automatically be updated for all of the applications.

Adapter for SiteMinder

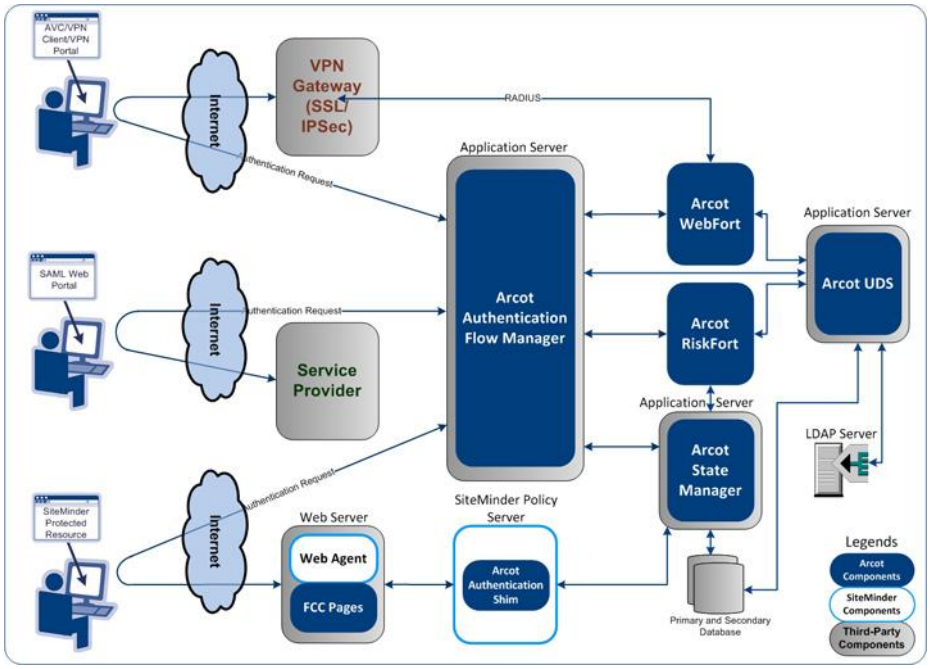
CA SiteMinder provides centralized security management capability that enables customers, partners, and end users to securely access and deliver applications and data on the Web. Integrating SiteMinder with Adapter allows you to protect your resources with multi-factor and risk-based adaptive authentication.

Adapter for VPN

Organizations provide their employees, contractors, and business partners with secure remote access by using VPN over existing internet connections. However, VPNs do not strongly defend against unauthorized access to the organization's electronic assets. Security experts recommend strong, two-factor authentication to protect remote access. Adapter can be easily integrated with VPNs to provide a solution that combines flexible, software-based strong authentication with a full-featured IPSec or SSL-based VPN system that does not change the user's login experience. The SSL-based VPN integration leverages all the authentication mechanisms supported by AuthMinder. However, the IPSec VPN integration supports only ArcotID PKI, which is CA's unique software-based credential.

Adapter Architecture

The following figure illustrates how Adapter components integrate with the supported applications.



As illustrated in this figure, Adapter includes the following *common* components:

- Authentication Flow Manager (see page 14)
- State Manager (see page 17)
- User Data Service (see page 17)

The following components are used for the SiteMinder integration:

- Authentication Shim (see page 18)
- Form Credential Collector (FCC) Pages (see page 18)

Adapter also uses "VPN Client" (see page 18) for the IPsec VPN integration. In addition, Adapter uses other advanced authentication products, which are explained in the section "Other Authentication Products Used with Adapter" (see page 18).

Authentication Flow Manager

Authentication Flow Manager (AFM) functions as an interface between users and other components of Adapter. For SAML-based portals, AFM can be deployed as an *Identity Provider* (IdP) providing SSO-based federated identity services using SAML 2.0. It also performs the function of a state machine that guides the end user through authentication workflows.

AFM provides you the flexibility to create common ready-to-use authentication configurations, known as *AFM profiles.* For more information about AFM profiles, see Understanding the AFM Profile (see page 48).

You can use AFM to configure the following out-of-the-box workflows:

Important! All workflows are capable of enrolling users who do not possess an AuthMinder credential.

- **Risk Evaluation and ArcotID PKI Authentication**: This authentication workflow is a combination of the risk evaluation and ArcotID PKI authentication workflows. This workflow can also be configured to use QnA, OTP by SMS, OTP by email, or ArcotID OTP on mobile phones for secondary authentication on SAML, SiteMinder, and SSL VPN integrations.
- **ArcotID PKI Authentication**: This workflow includes ArcotID PKI authentication using CA AuthMinder. This workflow can be configured to present QnA, OTP by SMS, OTP by email, or ArcotID OTP on mobile phones for secondary authentication on SAML, SiteMinder, and SSL VPN integrations. However, the IPsec VPN integration uses only QnA for secondary authentication.
- **LDAP and ArcotID PKI Authentication**: This workflow combines the LDAP or basic SiteMinder authentication scheme and ArcotID PKI authentication. In this workflow, the LDAP or basic authentication is performed before ArcotID PKI authentication. This workflow can be configured to present QnA, OTP by E-Mail, OTP by SMS, or ArcotID OTP on mobile phones for secondary authentication on a SiteMinder integration.
- **Risk Evaluation and LDAP Authentication:** This authentication workflow is a combination of the risk evaluation workflow and LDAP or basic SiteMinder authentication scheme. In this workflow, the risk evaluation is performed before the LDAP or basic authentication. This workflow can be configured to present QnA, OTP by SMS, OTP by email, or ArcotID OTP on mobile phones for secondary authentication on SAML, SiteMinder, and SSL VPN integrations.
- **LDAP Authentication and Risk Evaluation:** This authentication workflow combines the LDAP or basic SiteMinder authentication scheme and the risk evaluation workflow. In this workflow, the LDAP or basic authentication is performed before the risk evaluation. This workflow can be configured to present QnA, OTP by SMS, OTP by email, or ArcotID OTP on mobile phones for secondary authentication on SAML, SiteMinder, and SSL VPN integrations.

- **OATH-Based Authentication**: This workflow includes authentication using OATH-based hardware token credentials. You can configure this as a primary authentication mechanism for any supported application on SAML, SiteMinder, and SSL VPN integrations.
- **ArcotID OTP-Based Authentication for Mobiles and Other Devices**: This workflow includes authentication using ArcotID OTP. The OTP that is used for authentication is generated on your device, which can be a mobile device or the computer where the ArcotID OTP application is installed.

  You can configure this as a primary authentication mechanism for any supported application. You can also configure this workflow to present QnA, OTP by E-Mail, or OTP by SMS for secondary authentication on SAML, SiteMinder, and SSL VPN integrations.
- **Risk Evaluation and ArcotID OTP-Based Authentication for Browsers**: This workflow combines risk evaluation and ArcotID OTP authentication for browsers. In this workflow, risk evaluation is performed before the ArcotID OTP authentication. You can also configure this workflow to present QnA, OTP by E-Mail, or OTP by SMS for secondary authentication on SAML, SiteMinder, and SSL VPN integrations.
- **ArcotID OTP-Based Authentication for Browsers**: This workflow includes authentication using ArcotOTP for browsers. You can configure this as a primary authentication mechanism for any supported application.You can also configure this workflow to present QnA, OTP by E-Mail, or OTP by SMS for secondary authentication on SAML, SiteMinder, and SSL VPN integrations.

Typically, these authentication workflows are rendered as *JavaServer Pages* (JSPs) that collect user information required for authentication. All authentication workflows support user migration. For example, if a user is not enrolled for ArcotID PKI authentication, then the user is taken through the enrollment workflow to complete the authentication process.

The following JSP file can be used to directly enroll a user for AuthMinder authentication:

- **masterEnrollment.jsp**: The workflow defined in this JSP enrolls the user for the configured AuthMinder credentials. This is done after authenticating the user with LDAP, OTP, or both, depending on the configuration. If a profile has been configured in the AFM wizard, then to enroll the user for the credentials configured in the profile, a request parameter must be sent to the masterEnrollment.jsp file in the following format:

  arcotafm/masterEnrollment.jsp?profile=*profile-name*

  Note: This enrollment workflow is available at the following location: *application_server_home*/webapps/arcotafm/

  The following JSP file can be used to update the user's details:

- **settings.jsp**: This JSP is used to enable end users to update their credentials. The workflow defined in this JSP updates the credentials of the user. When you integrate this JSP in your application, ensure that a link to this JSP is displayed to the end user only after successful authentication. Use the following format for the URL that leads to this JSP:

  /arcotafm/settings.jsp?profile=profile-name

  In the case of SiteMinder integration, this URL must be protected with the same authentication mechanism that has been configured for the resource that the user is trying to access.

AFM also maintains the state data of the user workflow, conducts AuthMinder authentication, and reads or writes RiskMinder Device ID information required by RiskMinder. In addition to using the authentication workflows shipped with AFM, you can customize an authentication workflow as per your organization's requirements.

Important! All users enrolled for authentication through any of the authentication workflows are assigned some **Custom Attributes**, which are accessible through the AuthMinder Administration Console. While fetching the user details in the Administration Console, you might see any of the following **Custom Attributes**:

- AOTPXML
- PAM_IMAGE
- OATH_SYNCHRONIZED

  If you find any of the above-mentioned **Custom Attribute** in the user details, you *must not edit or delete* the attribute. Doing so would result in unsuccessful user authentication or enrollment workflow.

For information about supported authentication mechanisms for the different integration types, see the table in Configuring Adapter by Using the Wizard (see page 50).

State Manager

State Manager is responsible for creating, maintaining, and tracking the tokens that are used to associate the authentication and risk status of a logon session across multiple Adapter components, and your application. The tokens, which contain information about the user and the session state, enable other Adapter components to remain stateless.

State Manager also provides a token validation mechanism to securely communicate the authentication result, the risk result (if configured), and the subsequent action to be performed by the IdP or Authentication Shim.

In the case of a SiteMinder integration, State Manager also acts as a proxy to RiskMinder by providing risk evaluation services to other authentication components. State Manager receives the risk evaluation input parameters from the calling application and passes them to RiskMinder. After the risk evaluation is complete, State Manager inserts the risk evaluation result into the token for further examination or processing by other components. Based on the implemented workflow, risk evaluation can be performed before or after user authentication. If the risk evaluation takes place after user authentication, the result of the user authentication is stored in the token and then the risk evaluation is performed.

In the case of a SAML integration, State Manager maintains session information of the authenticated user in a token.

In the case of an SSL VPN integration, State Manager is required when the primary authentication mechanism is ArcotID OTP for browsers. If the ArcotID OTP is used on multiple devices, State Manager is required to keep the ArcotID OTP data consistent with the data stored on the server.

Adapter provides database failover support for State Manager. If the primary database server is unavailable, State Manager can switch over to the secondary database server. To use this feature, you need to configure the secondary database server and synchronize it with the primary database. This makes the 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 that you would need to configure. For details on the parameters that you need to configure to enable the database failover, see the table on Database Connectivity Parameters in Configuration Files and Options (see page 119).

User Data Service

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

Authentication Shim

Authentication Shim, which integrates with SiteMinder, acts as an interface between SiteMinder and other Adapter components (State Manager and AFM), and other products (AuthMinder and RiskMinder).

The Authentication Shim is an instance of a shared library and resides in the SiteMinder Policy Server instance. The Authentication Shim implements the SiteMinder Authentication API.

Form Credential Collector (FCC) Pages

FCC (referred to as FCC later in the guide) pages are static HTML pages used by Authentication Shim (see page 18) to collect user inputs during enrollment or basic authentication and to display error messages, if any. These pages are deployed on the same Web server where the SiteMinder Web Agent resides.

VPN Client

For IPSec VPN integration, Adapter uses the *CA VPN Client* application. This application is installed on the end-user's system. VPN Client works with AFM and AuthMinder Server to authenticate the end users before allowing them access to the resources available on the enterprise network. In case of IPSec VPN integration, VPN Client is the only component of Adapter that the end users interact with directly.

When a user specifies the ArcotID PKI credentials (user name and password), VPN Client interacts with Authentication Flow Manager (see page 14) for the ArcotID PKI authentication through AuthMinder. After successful authentication, AFM returns a *One-Time-Token* (OTT) to VPN Client which, in turn, invokes the client application of the VPN appliance and passes the user name along with the OTT for further processing.

Other Authentication Products Used with Adapter

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

- CA AuthMinder (see page 19)
- CA RiskMinder (see page 19)

AuthMinder

CA AuthMinder 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 any access manager by adding a transparent layer of strong multi-factor authentication.

Note: For information on installing and configuring AuthMinder, refer to the documentation shipped with that product.

RiskMinder

RiskMinder 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 network security personnel need to be notified.

Note: For information on installing and configuring RiskMinder, refer to the documentation shipped with that product.

Adapter Workflows

This section explains the end-user workflows, as experienced by the end users after they start using the integrated solution. This section describes the following workflows:

- End User Login Workflow in SAML (see page 20)
- End User Authentication Workflow in SiteMinder (see page 21)
- End User Authentication Workflow in IPSec VPN (see page 21)
- End User Authentication Workflow in SSL VPN (see page 22)

End User Login Workflow in SAML

The following steps explain the user authentication procedure when Adapter is integrated with any SAML-based Web portal:

1. The user accesses a Web portal containing links to various resources or applications.
2. The user clicks a link to access an application (for example, a banking application), which is hosted on the *Service Provider's* (SP) secure network.
3. The SP issues a SAML authentication request message, which is sent through the user's browser to the intended IdP using the HTTP Redirect method.
4. The IdP parses the SAML request and proceeds with user authentication, which could be configured to be authentication only or a combination of AuthMinder authentication and risk evaluation.
5. On successful authentication, AFM sends a request to State Manager for token creation. State Manager saves the user's state as a token and securely communicates the token information to the IdP.
6. The IdP securely communicates the authenticated SAML response through the user's browser (using HTTP POST) to the SP.
7. The SP validates the SAML response by using an appropriate certificate.
8. The SP grants access to the requested resource.

The user can now access any other application on the Web portal without logging in again.

End User Authentication Workflow in SiteMinder

The following steps explain the user authentication and risk assessment procedure when Adapter is integrated with SiteMinder and risk assessment is enabled:

1. The user accesses a resource that is protected by SiteMinder.
2. SiteMinder disambiguates the user.
3. If the authentication has to be performed by Arcot components, then Authentication Shim (see page 18) redirects the user to Authentication Flow Manager (see page 14).

   Note: If the user is not enrolled for AuthMinder authentication, AFM can be configured to take the user through the enrollment process.
4. AFM guides the user through the authentication and risk evaluation process, if risk assessment is configured.
5. Depending on the authentication and risk evaluation results, State Manager (see page 17) saves the user's state in a token and securely communicates the user's state along with the authentication and risk result to Authentication Shim.
6. Authentication Shim evaluates and forwards the authentication result to SiteMinder.

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

End User Authentication Workflow in IPSec VPN

A generic user authentication workflow after integrating Adapter with the Cisco IPSec VPN appliance is as follows:

1. User invokes VPN Client to connect to your enterprise network.
2. In the VPN Client user interface, user specifies their ArcotID PKI credentials and clicks the **Login** button to connect.
3. AFM performs ArcotID PKI authentication and returns an OTT to VPN Client.
4. VPN Client invokes the Cisco VPN client application, which, in turn, connects to the Cisco VPN server with the user's information and the OTT.
5. Cisco VPN server validates the OTT with AuthMinder, which is set up as the RADIUS server.
6. On successful authentication, user is logged in to your enterprise network.

End User Authentication Workflow in SSL VPN

A generic user authentication workflow after integrating Adapter with Juniper SSL VPN appliance is as follows:

1. User accesses the VPN login URL.
2. The user request is intercepted by the Juniper SSL VPN appliance, which, in turn, redirects the user request to AFM for authentication.
3. AFM along with AuthMinder authentication server completes the authentication.

   Note: ArcotID PKI and ArcotID PKI PIN that are a part of ArcotID PKI authentication are used to extract the private key of the user. This private key is then used to sign the challenge. Refer to *CA AuthMinder Installation and Deployment Guide* for more information on ArcotID PKI authentication.
4. AFM redirects the generated Authentication OTT to Juniper SSL VPN appliance.
5. Juniper SSL VPN appliance validates the OTT with AuthMinder, which is set up as the RADIUS server.
6. After successful user authentication, Juniper SSL VPN appliance provides access to the network.

Adapter Features

The key features and enhancements in the Adapter 2.2.9 release have been discussed in detail in the section, "What's New in this Release" in *CA Adapter Release Notes*.

Chapter 2: Planning the Deployment

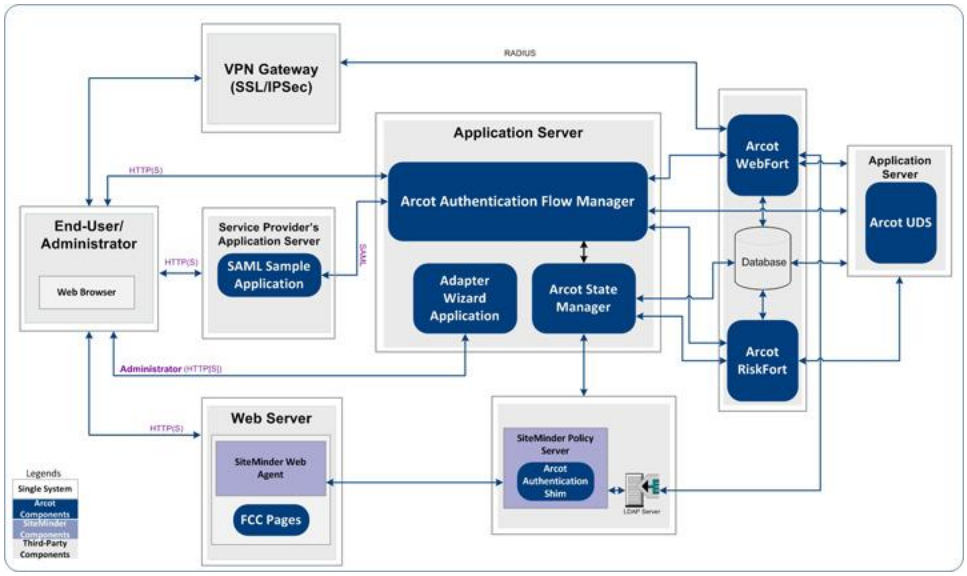
This chapter discusses the various deployment options for Adapter and helps you plan the deployment.

The following topics are covered in this chapter:

- Deployment Architecture (see page 23)
- Deployment Overview (see page 25)

Deployment Architecture

The following figure depicts a *possible* deployment option for prerequisite software and Adapter components.



Install and deploy Adapter components as depicted in this figure. Also, it is recommended that you use a secured communication channel between all Adapter components. For more information about configuring SSL communication, see "Configuring SSL in Apache Tomcat" (see page 173).

Important! As the systems involved in the deployment process must be accessed using their *Fully Qualified Distinguished Name* (FQDN) only, make the following changes:

- Ensure that you have added the Service Provider's IP address and Web server's IP address in the Windows **hosts** file of the end-user's system.
- Ensure that you have added the AFM application server's IP address in the Solaris and Linux **hosts** file of the Service Provider's system.

Deployment Overview

The following table serves as a checklist for installing Adapter for different types of integrations.

Integrating Adapter With	Steps to Complete
SiteMinder	1. Ensure that all the prerequisite software is installed and the database is set up, as described in Preparing for Installation (see page 29). 2. Install Adapter, as described in Installing Adapter (see page 37). 3. Deploy the Arcot Adapter Wizard application, as described in Deploying the Wizard (see page 49). 4. Configure AFM by using the wizard, as described in Configuring Adapter by Using the Wizard (see page 50). 5. Copy the Adapter configuration files, as described in Copying the Adapter Configuration Files (see page 64). 6. (Optional) Configure SSL for Apache Tomcat, as described in Configuring SSL in Apache Tomcat (see page 173). 7. Deploy State Manager and configure the database connection pooling, as described in Deploying and Configuring State Manager (see page 67). 8. Deploy Authentication Flow Manager, as described in Deploying and Configuring Authentication Flow Manager (see page 81). 9. Deploy FCC pages and Authentication Shim, as described in Configuring Authentication Shim and FCC Pages (see page 87). 10. Configure CA SiteMinder Policy Server and Web Agent, as described in Configuring CA SiteMinder Policy Server (see page 89). 11. Verify the State Manager configuration, as described in Verifying the State Manager Configuration (see page 103). 12. Verify the AFM configuration, as described in Verifying the AFM Configuration (see page 104). 13. Verify the Authentication Shim configuration, as described in Verifying the Authentication Shim Configuration (see page 104). 14. Verify the SiteMinder integration, as described in Verifying SiteMinder Integration (see page 105).

Integrating Adapter With	Steps to Complete
SAML	1. Ensure that all the prerequisite software is installed and the database is set up, as described in Preparing for Installation (see page 29). 2. Install Adapter, as described in Installing Adapter (see page 37). 3. Deploy the Arcot Adapter Wizard application, as described in Deploying the Wizard (see page 49). 4. Configure AFM by using the wizard, as described in Configuring Adapter by Using the Wizard (see page 50). 5. Copy the Adapter configuration files, as described in Copying the Adapter Configuration Files (see page 64). 6. Configure SSL for Apache Tomcat, as described in Configuring SSL in Apache Tomcat (see page 173). 7. Deploy State Manager and configure the database connection pooling, as described in Deploying and Configuring State Manager (see page 67). 8. Deploy Authentication Flow Manager, as described in Deploying and Configuring Authentication Flow Manager (see page 81). 9. Deploy the SAML sample application, as described in Deploying the Sample Application WAR Files (see page 93). 10. Verify the SAML sample application deployment, as described in Verifying the Sample Application Deployment (see page 97). 11. Configure the SAML sample application, as described in Configuring Sample Application (see page 97). 12. Verify the State Manager configuration, as described in Verifying the State Manager Configuration (see page 103). 13. Verify the AFM configuration, as described in Verifying the AFM Configuration (see page 104). 14. Verify SAML integration, as described in Verifying SAML Integration (see page 105).

Integrating Adapter With	Steps to Complete
Juniper SSL VPN	1. Ensure that all the prerequisite software is installed and the database is set up, as described in Preparing for Installation (see page 29). 2. Install Adapter, as described in Installing Adapter (see page 37). 3. Deploy the Arcot Adapter Wizard application, as described in Deploying the Wizard (see page 49). 4. Configure AFM by using the wizard, as described in Configuring Adapter by Using the Wizard (see page 50). 5. Copy the Adapter configuration files, as described in Copying the Adapter Configuration Files (see page 64). 6. Configure SSL for Apache Tomcat, as described in Configuring SSL in Apache Tomcat (see page 173). 7. (If Arcot ID OTP on Browser is the authentication mechanism) Deploy State Manager and configure the database connection pooling, as described in Deploying and Configuring State Manager (see page 67). 8. Deploy Authentication Flow Manager, as described in Deploying and Configuring Authentication Flow Manager (see page 81). 9. Perform the post-installation configuration and verification tasks described in the *CA Adapter for Juniper SSL VPN Configuration Guide*.

Integrating Adapter With	Steps to Complete
Cisco IPSec VPN	1. Ensure that all the prerequisite software is installed and the database is set up, as described in Preparing for Installation (see page 29). 2. Install Adapter, as described in Installing Adapter (see page 37). 3. Deploy the Arcot Adapter Wizard application, as described in Deploying the Wizard (see page 49). 4. Configure AFM by using the wizard, as described in Configuring Adapter by Using the Wizard (see page 50). 5. Copy the Adapter configuration files, as described in Copying the Adapter Configuration Files (see page 64). 6. Configure SSL in Apache Tomcat, as described in Configuring SSL in Apache Tomcat (see page 173). 7. Deploy Authentication Flow Manager, as described in Deploying and Configuring Authentication Flow Manager (see page 81). 8. Perform the post-installation configuration and verification tasks described in the *CA Adapter for Cisco IPSec VPN Configuration Guide*.

Chapter 3: Preparing for Installation

This chapter lists the software requirements for installing Adapter and discusses other prerequisites for SAML, SiteMinder, and VPN appliances. The following topics are covered in this chapter:

- Software Requirements for State Manager (see page 29)
- Software Requirements for Authentication Flow Manager (see page 31)
- Software Requirements for Authentication Shim (see page 33)
- Software Requirements for FCC Pages (see page 33)
- Checklist for Integration (see page 34)

Software Requirements for State Manager

Note: State Manager is required when Adapter is integrated with SAML-based Web portal, SiteMinder, or SSL VPN appliances (if the primary authentication mechanism is ArcotID OTP on Browser). You *do not* need to perform the instructions in this section if you are integrating Adapter with IPSec VPN appliances.

This section lists the prerequisites for installing State Manager. This section includes the following topics:

- Minimum Software Requirements (see page 29)
- Configuring the Application Server (see page 31)

Minimum Software Requirements

The following table lists the operating system requirements for State Manager.

Supported Operating System
Red Hat Enterprise Linux 5.4 (32-bit)
Red Hat Enterprise Linux 5.4 (64-bit)
Red Hat Enterprise Linux 6.1 (32-bit)
Red Hat Enterprise Linux 6.1 (64-bit)
Red Hat Enterprise Linux 6.2 (32-bit)
Red Hat Enterprise Linux 6.2 (64-bit)
Solaris 10 (SPARC)

If you want to enable risk evaluation, then before you deploy and configure State Manager, ensure that a supported version of the software listed in the following table is installed and configured.

Software	Supported Version	Supported Operating System
CA RiskMinder	3.1.01	Solaris 10 (SPARC) For more information, see the CA Advanced Authentication Compatibility Matrix.
or		
CA RiskMinder	3.1.01	Red Hat Enterprise Linux For more information, see the CA Advanced Authentication Compatibility Matrix.

Database Requirements

The following table lists the database requirements for State Manager.

Database Server
■ Microsoft SQL Server 2005 ■ Microsoft SQL Server 2008
■ MySQL Enterprise Edition 5.1
■ Oracle 10g ■ Oracle 11*g*

JDK and Application Server Requirements

The following table lists the minimum JDK and the application server requirements for State Manager. Both 32-bit and 64-bit versions of the application servers are supported.

Application Server	JDK
Apache Tomcat 5.5.31	Compatible versions of Oracle JDK. For more information, see the Apache Tomcat documentation.
Apache Tomcat 6.0.33	Compatible versions of Oracle JDK. For more information, see the Apache Tomcat documentation.
Apache Tomcat 7.0.25	Compatible versions of Oracle JDK. For more information, see the Apache Tomcat documentation.

Application Server	JDK
IBM WebSphere Application Server 6.1.0.41	IBM JDK 1.5.x
IBM WebSphere Application Server 7.0.x	IBM JDK 1.6.0
Oracle WebLogic 10.1.x	Oracle JRockIt 1.5.x
Oracle WebLogic 11gR1 or 10.3.3	Oracle JRockIt 1.6.x
JBoss Application Server 5.1.x	Oracle JDK 5.0

Configuring the Application Server

State Manager is a Web application that requires a Servlet container for its deployment. Because State Manager uses JNDI to connect to the database, you must create a JNDI connection. For more information, see Creating a JNDI Connection (see page 70).

It is recommended that State Manager communicate with other components using SSL mode. To configure State Manager for SSL, enable the application server on which State Manager is deployed for SSL communication.

Adapter provides sample Keystore and Truststore, which you can use for testing SSL communication between the Adapter Components.

Software Requirements for Authentication Flow Manager

The following table lists the operating system requirements for AFM.

Supported Operating System
Red Hat Enterprise Linux 5 (32-bit and 64-bit)
Red Hat Enterprise Linux 6 (32-bit and 64-bit)
Solaris 10 (SPARC)

Before deploying and configuring AFM, ensure that a supported version of the software listed in the following table is installed and configured.

Software	Supported Version	Supported Operating System
CA AuthMinder	7.1.01	Solaris 10 (SPARC) For more information, see the CA Advanced Authentication Compatibility Matrix.

Software	Supported Version	Supported Operating System
or		
CA AuthMinder	7.1.01	Red Hat Enterprise Linux 5 (32-bit and 64-bit) Red Hat Enterprise Linux 6 (32-bit and 64-bit) For more information, see the CA Advanced Authentication Compatibility Matrix.

Note: For more information about installing CA AuthMinder, see the *CA AuthMinder Installation and Deployment Guide*.

JDK and Application Server Requirements

The following table lists the JDK and the application server requirements for AFM. Both 32-bit and 64-bit versions of the application servers are supported.

Application Server	JDK
Apache Tomcat 5.5.31	Compatible versions of Oracle JDK. For more information, see the Apache Tomcat documentation.
Apache Tomcat 6.0.33	Compatible versions of Oracle JDK. For more information, see the Apache Tomcat documentation.
Apache Tomcat 7.0.25	Compatible versions of Oracle JDK. For more information, see the Apache Tomcat documentation.
IBM WebSphere Application Server 6.1.0.41	IBM JDK 1.5.x
IBM WebSphere Application Server 7.0.x	IBM JDK 1.6.0
Oracle WebLogic 10.1.x	Oracle JRockIt 1.5.x
Oracle WebLogic 11gR1 or 10.3.3	Oracle JRockIt 1.6.x
JBoss Application Server 5.1.x	Oracle JDK 5.0

Software Requirements for Authentication Shim

Note: The software requirements specified in this section are applicable *only* for SiteMinder integration.

Before proceeding with the Authentication Shim installation, ensure that a supported version of the software listed in the following table is installed and configured.

Software	Supported Version	Supported Operating System
CA SiteMinder Policy Server	■ r6.0 SP6 ■ r12.0 SP3 ■ r12.5	Solaris 10 (SPARC) (64-bit) For more information about the supported operating systems, see the SiteMinder Platform Support Matrix
or		
CA SiteMinder Policy Server	■ r6.0 SP6 ■ r12.0 SP3 ■ r12.5	Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6 For more information about the supported operating systems, see the SiteMinder Platform Support Matrix

Software Requirements for FCC Pages

Note: The software requirements specified in this section are applicable *only* for SiteMinder integration.

Before configuring the FCC pages, ensure that a supported version of the software listed in the following table is installed and configured.

Software	Supported Version	Supported Operating System
CA SiteMinder Web Agent	Refer to CA SiteMinder documentation for more information on the compatible Web Agent version.	For more information about the supported operating systems, see the SiteMinder Platform Support Matrix.

Checklist for Integration

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

- All prerequisite software are installed
  - CA AuthMinder 7.1.01 is installed on the required operating system.

    Note: For installing AuthMinder, see the *CA AuthMinder Installation and Deployment Guide*.
  - If risk evaluation support is needed, then Arcot RiskMinder is installed on the required operating system.

    Note: For installing RiskMinder, see the *CA RiskMinder Installation and Deployment Guide*.
- The application server(s) where you intend to deploy Adapter components are independently operational.
- The Web browser that you intend to use is configured to allow file download, active scripting, and scripting of Java applet functions.
- Required numbers of database instances are ready with applicable schemas for storing the information required by Adapter.
- The required number of the IPSec or SSL VPN appliances have been installed and configured.

The following additional requirements are needed for integrating Adapter with SiteMinder:

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

  Refer to the appropriate SiteMinder documentation for installation details.
- Create a virtual directory, for example, **arcotlogin**, on the Web server where you plan to install the FCC pages.

  Note: Note down the virtual directory name as you need this information at the time of configuring the FCC virtual directory path in the Adapter Configuration wizard.
- Create at least one object of the following types by using the SiteMinder Policy Server User Interface (r6.x) or Administrative User Interface (r12.x), as applicable. 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 4: Installing Adapter

This chapter walks you through the process of installing Adapter on Solaris and Linux platforms, so that you can use credentials based on any AFM profile with SAML, SiteMinder, or VPN appliance. Adapter can also be configured to provide risk evaluation feature for SAML and SiteMinder integrations.

Important!

- It is assumed that you are installing Adapter and its components on a fresh system. The system where you plan to deploy Adapter *must not* have any previous installation of Adapter or any of its components.
- If you are installing Adapter and other authentication products (AuthMinder or RiskMinder) on the same system in the same location, then you must install these products *before* installing Adapter.

Use the Adapter 2.2.9 installation wizard to install Adapter and its components. This Wizard supports Complete and Customize installation types. After performing the installation, you can check whether the installation has been performed successfully. This chapter covers the following topics:

- Installing in a Distributed Environment (see page 37)
- Installing on a Single System (see page 44)
- Verifying the Installation (see page 45)

Note: This chapter does not cover the installation procedure for prerequisite software that are depicted in the deployment architecture diagram (see page 23).

Installing in a Distributed Environment

To install and configure Adapter in a distributed environment, you must use the **Customize** option when you run the installer. This section describes the steps that you must follow to install Adapter components for the following integration types:

- For SiteMinder Integration (see page 38)
- For SAML Integration (see page 41)
- For VPN Integration (see page 43)

Note: Before proceeding with the installation, ensure that all the prerequisite software is installed and the database is set up, as described in Preparing for Installation (see page 29).

For SiteMinder Integration

Before proceeding with the installation, refer to the deployment architecture. This diagram illustrates the components that are required for each integration type, and also helps you decide how you want to distribute the components. For SiteMinder Integration, you must install the components listed in the following table.

Components	Description
Authentication Flow Manager and Related Components (see Installing Common Adapter Components (see page 39)) **Note:** You can install Authentication Flow Manager (AFM), AFM Wizard, and State Manager components on a fresh system that hosts your application server.	
Authentication Flow Manager	Navigates the user through the authentication process, risk evaluation process, or both.
AFM Wizard	A Web-based application that helps perform basic configurations of other Adapter components.
State Manager	Generates, maintains, and tracks the tokens that are used to associate the authentication and risk status of users' sessions across Adapter and the integrated solution's components.
Components on SiteMinder Policy Server System (see Installing on SiteMinder Policy Server System (see page 41))	
Authentication Shim	This is the core component of the integrated solution. It enables interaction between Arcot components, SiteMinder, and other authentication schemes.
Components on SiteMinder Web Agent System (see Installing on SiteMinder Web Agent System (see page 41))	
Form Credential Collector Pages	Collects authentication input from the user and sends it for authentication and risk evaluation.

Installing Common Adapter Components

To install Authentication Flow Manager (AFM), AFM Wizard, and State Manager components:

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

   prompt> mkdir /tmp_install
3. Copy the Adapter installer file to the temporary directory that you created in Step 2, using the following command:

   - **For Solaris:**
     prompt> cp **Arcot-Adapter-2.2.9-Solaris.tar.gz** /tmp_install
   - **For Linux:**
     prompt> cp **Arcot-Adapter-2.2.9-RHEL.zip** /tmp_install
4. Unzip the installer file as shown in the following example:

   - **For Solaris:**
     prompt> cd /tmp_install
     prompt> gzip –d Arcot-Adapter-2.2.9-Solaris.tar.gz
   - **For Linux:**
     prompt> cd /tmp_install
     prompt> unzip Arcot-Adapter-2.2.9-RHEL.zip
5. (*For Solaris*) Extract the TAR file, using the following command:
   prompt> tar –xvf Arcot-Adapter-2.2.9-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-2.2.9-Solaris-Installer.bin
7. Run the installation wizard by using the following command:
   prompt> sh Arcot-Adapter-2.2.9-*platform name*-Installer.bin

   Note: If you are executing the installer with root login, the following warning message opens:

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

   The License Agreement for Adapter opens.
9. On the License Agreement screen:

   Read the text carefully and press **Enter** to display the next screen of the license text. You might have to press **Enter** multiple times, until the entire text for License Agreement is displayed.

At the end of the license agreement, you will be prompted for acceptance of the terms of license agreement (**DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT?**).

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 opens.

11. As directed on the screen, you can *either*:

    - Enter the absolute path of the directory where you want to install Adapter and press **Enter** to continue.

      Note: The installation directory name that you specify *must not* contain any spaces. Else, some Adapter scripts and tools might not function as intended.

    - Press **Enter** to accept the default directory displayed by the installer.

    The Choose Install Type screen opens.

12. Type **2** and press **Enter** to accept the **Customize** installation option and to continue with the installation.

    The Choose Product Features screen opens. This screen enables you to select the specific components that you wish to install on the system.

13. Specify a comma-separated list (*without any space between the comma and the number*) of numbers representing the Adapter components that you *do not* want to install on the current system. Only the following components must be installed.

    - AFM Wizard
    - Authentication Flow Manager
    - State Manager

14. Press **Enter** to continue.

    The Pre-Installation Summary screen opens. This screen lists the product details, installation directory, type of installation, and components that are to be installed.

15. Review the product details displayed carefully and press **Enter** to proceed with the installation. If you would like to change a configuration on any of the previous screens, type **back** until you reach the screen, make the required changes, and press **Enter** to proceed to the next screen.

    The Ready to Install screen opens.

16. Press **Enter** to continue.

    The Installing screen opens, 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 opens.

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

Installing on SiteMinder Policy Server System

To install Adapter components on the system where SiteMinder Policy Server is installed:

1. Follow the instructions from Step 1 to Step 12, as discussed in For SiteMinder Integration (see page 38) section to reach the **Choose Product Features** screen.
2. Install only the **Authentication Shim** component.

   The installer creates a folder called **arcot** in the installation location, and includes the Adapter files in this folder.
3. Perform the tasks in Step 14 to Step 17, as discussed in For SiteMinder Integration (see page 38) section to complete the installation.

Installing on SiteMinder Web Agent System

To install Adapter components on the system where SiteMinder Web Agent is installed:

1. Follow the step instructions from Step 1 to Step 12, as discussed in For SiteMinder Integration (see page 38) to reach the **Choose Product Features** screen.
2. Install only the **Form Credential Collector Pages** component.

   The installer creates a folder called **arcot** in the installation location, and includes the Adapter files in this folder.
3. Perform the tasks in Step 14 to Step 17, as discussed in For SiteMinder Integration (see page 38) to complete the installation.

For SAML Integration

Before proceeding with the installation, refer to the deployment architecture diagram. That diagram illustrates the components that are required for each integration type, and also helps you decide how you want to distribute the components.

For SAML Integration, you must install the components listed in the following table.

Components	Description
Authentication Flow Manager and Related Components (see Installing Common Adapter Components (see page 42)) **Note:** You can install Authentication Flow Manager (AFM), AFM Wizard, and State Manager components on a fresh system that hosts your application server.	
Authentication Flow Manager	Navigates the user through the authentication process, risk evaluation process, or both.
AFM Wizard	A Web-based application that helps perform basic configurations of other Adapter components.

Components	Description
State Manager	Generates, maintains, and tracks the tokens that are used to associate the authentication and risk status of users' session across Adapter and integrated solution's components.
	Components on Service Provider's System (see Installing on Service Provider's System (see page 42))
Sample Applications	A set of three sample applications that you can use to test the SAML integration.

Installing Common Adapter Components

The instructions for installing AFM, AFM Wizard, and State Manager are the same as those discussed in Installing Common Adapter Components (see page 39) For SiteMinder Integration (see page 38)

Installing on Service Provider's System

To install SAML sample applications on the Service Provider's system:

1. Follow the step instructions from Step 1 to Step 12, as discussed in Installing Common Adapter Components (see page 39) For SiteMinder Integration (see page 38) to reach the **Choose Product Features** screen.
2. Install only the **Sample Applications** component.

   The installer creates a folder called **arcot** in the installation location, and includes the Adapter files in this folder.
3. Perform the tasks in Step 14 to Step 17, as discussed in Installing Common Adapter Components (see page 39) For SiteMinder Integration (see page 38) to complete the installation.

For VPN Integration

Before proceeding with the installation, refer to the deployment architecture diagram. That diagram illustrates the components that are required for each integration type, and also helps you decide how you want to distribute the components.

For VPN Integration, you must install the components listed in the following table.

Components	Description
Authentication Flow Manager and Related Components (see Installing Common Adapter Components (see page 44)) **Note:** You can install Authentication Flow Manager (AFM), AFM Wizard, and State Manager components on a fresh system that hosts your application server.	
AFM Wizard	A Web-based application that helps perform basic configurations of other Adapter components.
Authentication Flow Manager	Navigates the user through the authentication process, risk evaluation process, or both.
Important! State Manager is required only when you are integrating Adapter with an SSL VPN solution that you plan to use with the ArcotID OTP on Browser authentication mechanism. You *do not* need to configure State Manager for IPsec VPN integration.	
State Manager	Generates, maintains, and tracks the tokens that are used to associate the authentication and risk status of users' session across Adapter and integrated solution's components.

Installing Common Adapter Components

To install AFM, AFM Wizard, and State Manager:

1. Follow the step instructions from Step 1 to Step 12, as discussed in Installing Common Adapter Components (see page 39) For SiteMinder Integration (see page 38) to reach the **Choose Product Features** screen.
2. Specify a comma-separated list (*without any space between the comma and the number*) of numbers representing the Adapter components you *do not* want to install on the current system. Only the following components must be installed.
   - AFM Wizard
   - Authentication Flow Manager
   - *(Optional)* State Manager

   By default, all components are selected for installation. Deselect the components that are not required.

   The installer creates a folder called **arcot** in the installation location, and includes the Adapter files in this folder.
3. Perform the tasks in Step 14 to Step 17, as discussed in Installing Common Adapter Components (see page 39) For SiteMinder Integration (see page 38) to complete the installation.

Installing on a Single System

To install Adapter and its components on a single system, use the **Complete** installation type.

Note: The **Complete** installation type is applicable *only* for SiteMinder integration. *Do not* use this option for other integration types.

To install Adapter on a single system:

1. Follow the step instructions from Step 1 to Step 11 to reach the **Choose Install Type** screen.
2. Type **1** and to select the default (**Complete**) installation option.
3. Perform the tasks in Step 14 to Step 17 to complete the installation.

Note: Adapter also includes a Custom Application that can be used to test the authentication workflows without the need to integrate Adapter with any application. For more information about deploying and testing the workflows using the Custom Application, see Deploying and Configuring the Custom Application (see page 159).

Verifying the Installation

After installation, you can access the installation log file, **Arcot_Adapter_2.2.9_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.

If for some reason, the installation failed, then an error log is available in the same location from where you ran the installer.

Also, verify that the files listed in Adapter File System Structure (see page 111) are available on the system where you have installed Adapter.

Chapter 5: Performing Adapter Configuration Using the Wizard

Arcot Adapter Configuration wizard is a Web-based application used to configure authentication and enrollment workflows. By using the Arcot Adapter Configuration wizard, you can generate the configuration (.properties and .ini) files, which are used in the integrated solution.

The configurations in the wizard are grouped into two parts. In the first part, you need to create a profile, which controls the user's authentication and enrollment flows. The second part, referred to as *Configure Global Settings* enables you to configure the parameters specific to the type of integration option that you selected and the authentication mechanism configured for the profile.

The following table lists the sections available in the second part of the configuration wizard. The sections that you can access and configure in this part depend on the selected integration type and primary authentication mechanism.

Integration Type	Configurable Sections
SAML	■ Arcot WebFort and Arcot RiskFort Configuration ■ Arcot UDS Configuration ■ Arcot State Manager Configuration ■ SAML Configuration
SiteMinder	■ Arcot WebFort and Arcot RiskFort Configuration ■ Arcot UDS Configuration ■ Arcot State Manager Configuration ■ SiteMinder Shim Configuration
VPN	■ Arcot WebFort and Arcot RiskFort Configuration **Note:** Only in case of SSL VPN integration type and only if Perform Risk Assessment is selected, you need to *configure* the RiskMinder Server-related parameters in the Arcot WebFort/Arcot RiskFort Configuration section. The Perform Risk Assessment option is not available for integration of type IPSec VPN. ■ Arcot UDS Configuration ■ Arcot State Manager Configuration. This section is available only if AOTP on Browser is selected as the primary authentication mechanism in case of SSL VPN only.

Integration Type	Configurable Sections
All	■ Arcot WebFort and Arcot RiskFort Configuration ■ Arcot UDS Configuration ■ Arcot State Manager Configuration ■ SiteMinder Shim Configuration ■ SAML Configuration

This chapter covers the following topics:

- Understanding the AFM Profile (see page 48)
- Deploying the Wizard (see page 49)
- Configuring Adapter by Using the Wizard (see page 50)
- Copying the Adapter Configuration Files (see page 64)

Understanding the AFM Profile

Each end user in AFM is associated with at least one credential (such as ArcotID PKI, QnA, Password, or OTP) that they must use to log in to the application. Every time they log in using their credential, their authentication is controlled by a corresponding profile.

The AFM wizard provides you the flexibility to create common ready-to-use authentication configurations, known as *AFM profiles* that can be shared among multiple organizations and, thereby, applied to multiple users.AFM Profiles specify authentication configuration properties, and credential attributes such as, primary and secondary authentication mechanisms, validity period for the chosen credential, and how to enroll a new user.

You can create multiple profiles, each with a unique name. You can then assign one or more profiles to an organization, one of which can also be set as default. AFM makes use of these configured profiles at the time of authenticating or enrolling users.

Deploying the Wizard

To use the wizard, you first need to deploy the WAR file containing the wizard application. To deploy the WAR files:

Important! It is assumed that you will be deploying the Adapter components as depicted in Deployment Architecture (see page 23).

1. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory and restart your application server.
2. Navigate to the directory where the **ArcotAFMWizard.war** file is located. By default, this WAR file is available at the following location:

   afm_wizard_installation_dir/AFMWizard
3. Install ArcotAFMWizard.war on the system where you plan to deploy the AFM application.

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

   application_server_home/webapps

   Apache Tomcat automatically deploys the WAR file and creates a folder named ArcotAFMWizard under the webapps folder.

   Note: Refer to the vendor documentation for instructions on how deploy on other supported application servers.
4. Access the following URL from the end-user's system:

   http[s]://host_name:port-number/ArcotAFMWizard/

   Replace *host_name* and *port-number* with the host name and port of the system where you have deployed the Adapter Wizard application. You should see the Arcot Adapter Configuration Wizard page.

You can now use the wizard to create profiles, configure various components, and generate the configuration files. The following section guides you through the process of configuring the Adapter components by using the wizard.

Configuring Adapter by Using the Wizard

Perform the following steps to configure the Adapter components:

1. From the end-user's system, access the following URL:

   http[s]://*host_name*:*port*/ArcotAFMWizard/index.html

   The AFM Profiles screen opens.

2. Click the **Create new Profile** link.

   The AFM Profile Configuration screen opens.

3. Configure the parameters on the AFM Profile Configuration page.

   The following table describes the fields available on the AFM Profile Configuration page.

Section	Field	Description
AFM Profile Configuration	AFM Profile Name	Specify a name for the AFM profile. **Note:** You can enter a maximum of 16-digit alphanumeric characters in this field. Ensure that there are no special characters and blank space in your profile name.
	Integration Type	Select the type of integration that this profile should handle. The possible options are: ■ SiteMinder ■ SAML ■ SSL VPN ■ IPSec VPN **Note:** You can select multiple integration types by pressing the **Ctrl** key and selecting the required integration type.

Section	Field	Description
Primary Authentication Configuration	Primary Authentication	Select a primary authentication mechanism to use with this profile. The primary authentication mechanism you can configure depends on the integration type you selected in the **Integration Type** field. ■ **SiteMinder** supports the following types of primary authentication mechanisms: – ArcotID – LDAP – ArcotOTP on Browser – ArcotOTP on Mobile Device – OATH – LDAP + ArcotID ■ **SAML** and **SSL VPN** supports the following types of primary authentication mechanisms: – ArcotID – LDAP – ArcotOTP on Browser – ArcotOTP on Mobile Device – OATH ■ **IPSec VPN** supports *only* ArcotID as the primary authentication mechanism. **Note:** If you have selected *all* integration types, then ArcotID would become the default primary authentication mechanism.
WebFort Organization Name	WebFort Organization Name	Specify the AuthMinder organization name. If the specified organization does not exist in AuthMinder, then you must create it before testing the integrated solution. Select "**This organization is mapped to enterprise LDAP**" option, if the AuthMinder organization you specified is configured to use the LDAP repository. See Additional Configurations to Support LDAP Repository in AuthMinder (see page 165) for information about additional configurations to support LDAP repository in AuthMinder.

1. Click **Next**.

   Note: If you have not specified any organization name in the **Organization Name** field, then AuthMinder's default organization is used with this profile. A prompt appears asking whether the default organization is mapped with LDAP, if it is, then you must **Cancel** the prompt and select "**This organization is mapped to enterprise LDAP**" option before proceeding.

   Depending on the type of the Primary Authentication mechanism you selected in Step 3, the wizard will show you the configurable parameters applicable for that authentication mechanism. These parameters are grouped under various sections. The following table lists the configuration sections that you will see depending on the type of authentication mechanism you selected.

Primary Authentication	**Configurable Section**
ArcotID	■ Risk Assessment Configuration ■ General Configuration ■ ArcotID Configuration ■ Secondary Authentication Mechanism ■ Issuance Profile Configuration ■ Authentication Policy Configuration
LDAP	■ Risk Assessment Configuration ■ General Configuration ■ Secondary Authentication Mechanism ■ Issuance Profile Configuration ■ Authentication Policy Configuration
ArcotOTP on Browser	■ Risk Assessment Configuration ■ General Configuration ■ ArcotOTP Configuration ■ Secondary Authentication Mechanism ■ Issuance Profile Configuration ■ Authentication Policy Configuration
ArcotOTP on Mobile Device	■ General Configuration ■ ArcotOTP Configuration ■ Secondary Authentication Mechanism ■ Issuance Profile Configuration ■ Authentication Policy Configuration

Primary Authentication	Configurable Section
OATH	■ General Configuration ■ Issuance Profile Configuration ■ Authentication Policy Configuration
LDAP + ArcotID (SiteMinder only)	■ General Configuration ■ ArcotID Configuration ■ Secondary Authentication Mechanism ■ Issuance Profile Configuration ■ Authentication Policy Configuration

The following table describes the field available in the Risk Assessment Configuration section.

Field	Description
Perform Risk Assessment	Select this option to perform the risk assessment along with the selected primary authentication mechanism. If selected, then the following two options are made available: ■ **Pre-Authentication**: If this option is selected, the risk assessment is performed before the primary authentication. ■ **Post-Authentication**: If this option is selected, the risk assessment is performed after the primary authentication. **Note:** If ArcotID is selected as the primary authentication mechanism, then by default the risk assessment is performed before ArcotID authentication.

The following table describes the fields available in the General Configuration section.

Field	Description
Perform enrollment using an activation code	This option specifies the mechanism of sending the activation code to the user during enrollment. AFM performs enrollment on successful authentication of the activation code. By default this option is selected, you can select the mode of communication, which is email or SMS. This configuration is *optional* if the LDAP organization is selected as the AuthMinder organization. **Note:** If you choose to send the activation code through email, then you must configure the parameters in the "Email Server Configuration" section.
Log user into the system after successful enrollment	If selected, AFM considers the enrollment as authenticated and no explicit user authentication is required. If this option is not selected, users must authenticate themselves after enrollment.
Collect first name, middle name, and last name details during enrollment	If selected, users must enter their first, middle, and last names during enrollment. This configuration is *not applicable* if the configured organization is an LDAP organization.
Support for user-defined questions	Select this option to allow the user to add their own question that is not available in the existing list of out-of-the-box questions.
Enable email notification	If selected, AFM sends a notification email for different scenarios, such as successful enrollment, roaming download of ArcotID, password change, ArcotOTP on Mobile, ArcotOTP on Browser and updates to security questions, user details, and ArcotID password. **Note:** If you choose to send the notification email, then you must configure the parameters in the Email Server Configuration section.
Prompt user to accept cookies	Select this option to ask the user for permission to store cookies on their system.
Prompt user to enter his personal assurance message	Select this option to enable the user to enter a personal assurance message during enrollment. This message is presented to the user to assure them that they are interacting with the correct and legitimate server.

Field	Description
Prompt user to select personal assurance image	Select this option to enable the user to select an image during enrollment. This image is presented to the user to assure them that they are interacting with the correct and legitimate server.

The following table describes the fields available in the ArcotID Configuration section.

Field	Description
Allow users to be able to renew their ArcotID on expiry	Select this option to allow users to renew their impending ArcotID PKI credential.
Generate new ArcotID while renewal	Select this option if a new ArcotID PKI should be generated instead of renewing the existing ArcotID PKI.
ArcotID Renewal time period (in months)	Specify the time period for which the issued ArcotID PKI will be valid. **Note:** You cannot configure this field if **Generate new ArcotID while renewal** option is selected.
ArcotID Client Type and Preference	Select the ArcotID Client type to be used for authentication. If you select more than one option, then you can specify the order of preference for the ArcotID Client to be used. For example, if Flash is the first option in the list followed by JavaScript, then AFM checks for the availability of Flash in the user's browser. If AFM cannot detect Flash, it uses JavaScript as the client type for authentication. Possible options are: ■ JavaScript ■ Flash ■ Native **Note:** If you want to select Native as the preferred client type, then you must select **Native** in the list and click **Up** to move Native to the top of the list.

1. Click **Next**.

   Depending on the type of primary authentication mechanism you selected, you might see any or all of the following configuration sections.

   The following table describes the field available in the Secondary Authentication Mechanism section.

Section Name	Description
Secondary Authentication Mechanism	Select one or more of the secondary authentication mechanisms, such as **Security Question**, **OTP by Email**, **OTP by SMS**, and **ArcotOTP on Mobile** for different scenarios, such as **RiskFort Advice Increase Auth**, **Forgot Your Password**, **ArcotID Expiry**, and **ArcotID Roaming**. The default secondary authentication method is Security Questions. Secondary authentication is performed during roaming download, forgot password, and increase authentication scenarios. AFM allows you to select multiple secondary authentication mechanisms. **Note:** If you select the **OTP by Email** mechanism for secondary authentication, then you must configure the parameters in the "Email Server Configuration" section. If you select the **OTP by SMS** mechanism for secondary authentication, then you must configure the parameters in the "Clickatell SMS Service Configuration" section.

   The following table describes the fields available in the Issuance Profile Configuration section.

Field	Description
ArcotID Profile Name	The name of the ArcotID PKI profile created in AuthMinder that should be used at the time of creating or updating user credential.
Security Questions Profile Name	The name of the Security Question and Answer profile created in AuthMinder that should be used at the time of creating or updating the user credential.
OTP Profile Name for Secondary Authentication	The name of the OTP profile created in AuthMinder that should be used at the time of creating or updating the user credential.

Field	Description
ArcotOTP Profile Name	The name of the ArcotID OTP profile created in AuthMinder that should be used at the time of creating or updating the user credential.
OTP Profile Name for Enrollment Activation Code	The name of the OTP profile created in AuthMinder that should be used at the time of creating or updating user credential.

The following table describes the fields available in the Authentication Policy Configuration section.

Field	Description
ArcotID Policy Name	The name of the ArcotID PKI policy created in AuthMinder that should be used during authentication.
Security Questions Policy Name	The name of the Security Question and Answer policy created in AuthMinder that should be used during authentication.
OTP Policy Name for Secondary Authentication	The name of the OTP policy created in AuthMinder that should be used during authentication.
ArcotOTP Policy Name	The name of the ArcotID OTP policy created in AuthMinder that should be used during authentication.
OTP Policy Name for Enrollment Activation Code	The name of the OTP policy created in AuthMinder that should be used during authentication.

The following table describes the fields available in the ArcotID OTP Configuration section.

Field	Description
Allow users to be able to renew their ArcotOTP on expiry	Select this option to allow users to renew their impending ArcotID OTP.
Generate new ArcotOTP while renewal	Select this option if a new ArcotID OTP should be generated instead of renewing the existing ArcotID OTP.
ArcotOTP Renewal time period (in months)	Specify the time period for which the issued ArcotID OTP will be valid.

1. Click **Create**.

   The new profile details are saved and the profile name appears in the AFM Profiles page.

2. Click **Configure Global Settings**.

   The WebFort and RiskFort Configuration screen opens.

   Note: The RiskFort configuration section is displayed only if you enabled risk assessment when configuring the AFM profile.

   The following table describes the fields available in the WebFort and RiskFort Configuration page.

Section	Field	Description
WebFort Server Configuration	Authentication Host Name	Specify the *Fully Qualified Distinguished Name* (FQDN) of AuthMinder Server.
	Authentication Port	Specify the port at which AuthMinder Server is available. Default value: **9742**
	Issuance Host Name	Specify the FQDN of the server hosting the AuthMinder Issuance service.
	Issuance Port	Specify the port at which the server hosting the AuthMinder Issuance service is available. Default value: **9744**
RiskFort Server Configuration	DeviceID Storage Type	Select a mode to store the user's device ID information. The available options are: ■ HTTP Cookie ■ Flash Cookie
	Host Name	Specify the FQDN of RiskMinder Server.
	Port	Specify the port at which RiskMinder Server is available. Default value: **7680**

Note: If you are using secondary AuthMinder and RiskMinder servers, then specify the secondary servers details in the corresponding fields.

1. Click **Next**.

   The Arcot UDS Configuration screen opens.

   The following table describes the fields available in the Arcot UDS Configuration page.

Section	Field	Description
Arcot UDS Configurations	Protocol	Specify the protocol for connecting to UDS. The available options are: ■ HTTP ■ HTTPS
	Host Name	Specify the IP address or the FQDN of UDS.
	Port	Specify the port at which UDS is available.
	User Management Service URL pattern	Specify the URL pattern for UDS. Default value: **arcotuds/services/ArcotUserRegistrySvc**
Email Server Configuration	SMTP Host Name	Specify the FQDN or IP address of the server hosting the SMTP email service.
	SMTP Username	Specify the user name to access the SMTP email service.
	SMTP Password/ Confirm SMTP Password	Specify the password to access the SMTP email service.
Clickatell SMS Service Configuration	Clickatell Service URL	Specify the URL where Clickatell SMS service is available. Default value: http://api.clickatell.com/http/sendmsg?
	Clickatell API ID	Specify the unique identifier of the API that handle the SMS request.
	Clickatell Username	Specify the user name to access the Clickatell SMS service.
	Clickatell Password/ Confirm Clickatell Password	Specify the password to access the Clickatell SMS service.

1. Click **Next**.

   The Arcot State Manager Configuration screen opens.

   The following table describes the fields available in the Arcot State Manager Configuration page.

Section	Field	Description
Arcot State Manager Configuration	Protocol	Select the protocol for State Manager Server. **Note:** If you select HTTPS, then you must configure your application server for SSL communication. For more information about configuring SSL in Apache Tomcat, see Configuring SSL in Apache Tomcat (see page 173).
	Host Name	Specify the FQDN of State Manager Server.
	Port	Specify the port at which the application server hosting State Manager is available.
	Database Type	Specify the type of database to use with State Manager. Possible options are: ■ MS SQL Server ■ MySQL ■ Oracle
	Application Server	Select the application server on which State Manager is deployed. Possible options are: ■ Apache Tomcat ■ Oracle WebLogic ■ IBM WebSphere ■ JBoss
	Primary JNDI Name	Specify the JNDI name given to the primary database connection pool setup for the Sate Manager database.
	Secondary JNDI Name	Specify the JNDI name given to the secondary database connection pool setup for the Sate Manager database.

1. Click **Next**.

   The SiteMinder Shim Configuration screen opens.

   The following table describes the fields available in the SiteMinder Shim Configuration page.

Section	Field	Description
SiteMinder Web Agent Configuration	Protocol	Select the protocol for the Web server hosting SiteMinder Web Agent.
	Host Name	Specify the FQDN of the Web server where you have deployed the FCC pages.
	Port	Specify the port at which the Web server hosting SiteMinder Web Agent is available.
	FCC Virtual Directory	Specify the virtual directory name (for example, **arcotlogin**) created for deploying the FCC pages.
Application Server Configuration for AFM	Protocol	Select the protocol for the application server hosting the AFM application.
	Host Name	Specify the FQDN of the application server hosting the AFM application.
	Port	Specify the port at which the application server hosting the AFM application is available.

2. Click **Next**.

   The SAML Configuration screen opens.

   The following table describes the fields available in the SAML Configuration page.

   Note: In the SAML Request Verification Configuration section, you can configure either the **Certificate** or the **Truststore** details.

Section	Field	Description
SAML Request Verification Configuration	Certificate Location	Specify the absolute path of the X.509 certificate of the Service Provider. This is used to verify the signed SAML requests from the Service Provider. The corresponding key store must be used by the SAML sample application for signing the SAML request. **Note:** The certificate must be in .DER format.

Section	Field	Description
	Truststore Location	Specify the absolute path of the trust store file of the Service Provider. This file has a certificate that is used to verify the signed SAML requests from the Service Provider. The corresponding key store must be used by the SAML sample application for signing the SAML request.
	Truststore Alias	Specify the alias with which the certificate is stored in the truststore of the Service Provider.
	Truststore Password	Specify the password for the truststore of the Service Provider.
SAML Response Signing Configuration	Keystore Location	Specify the absolute or relative path of the Identity Provider's keystore file on the file system. This file has both the private key and certificate that are used for signing the SAML response. **Note:** Ensure that the public-private key pair is generated using "RSA" as the key algorithm and "SHA1withRSA" as the signing algorithm.
	Keystore Alias	Specify an alias of the private key and certificate stored in the Identity Provider's keystore.
	Keystore Password	Specify the password for the keystore of the Identity Provider.

3. Click **Next**.

   The Verify Input screen opens.

   Review the information on this screen, and if you need to change a previous selection, then click **Previous** to do so. After making the required changes, click **Next** to come back to the Verify Input page.

4. Click **Save**

   The wizard saves your settings and creates the configuration files at the following location:
   AFM_HOME/conf/afm

   Note: AFM_HOME is the environment variable that stores the Adapter install location. By default, Adapter is installed in the /opt/**arcot** directory.

   The following table lists the files that are generated for different types of integration.

Integration Type	Properties Files Generated
SAML	■ **arcotafm.properties** Contains the AFM configurations. ■ **saml_config.properties** Contains configurations for the SAML integration. ■ **samlsampleapp.properties** Contains the SAML sample application's configurations. ■ **arcotsm.properties** Contains the State Manager configurations.
SiteMinder	■ **arcotafm.properties** Contains the AFM configurations. ■ **adaptershim.ini** Contains the Authentication Shim-related configurations. ■ **arcotsm.properties** Contains the State Manager configurations.
VPN	■ **arcotafm.properties** Contains the AFM configurations. In addition to the above file, the following file will be created when **AOTP on Browser** is selected as the primary authentication mechanism: ■ **arcotsm.properties** Contains the State Manager configurations.

Integration Type	Properties Files Generated
All	■ **arcotafm.properties** Contains the AFM configurations. ■ **saml_config.properties** Contains configurations for the SAML integration. ■ **samlsampleapp.properties** Contains the SAML sample application configurations and the custom application configurations. ■ adaptershim.ini Contains the Authentication Shim-related configurations. ■ **arcotsm.properties** Contains the State Manager configurations. ■ **customapp.properties** Contains the custom application-related configurations.

Copying the Adapter Configuration Files

This section describes how to deploy the Adapter properties files for the following integration types:

- For SiteMinder Integration (see page 65)
- For SAML Integration (see page 65)
- For VPN Integration (see page 65)

For SiteMinder Integration

To deploy the properties files for SiteMinder integration:

1. Copy adaptershim.ini from *AFM_HOME*/conf/afm folder to the following location on the system where SiteMinder Policy Server is hosted:

   AFM_HOME/**conf**

   Note: *AFM_HOME* is the environment variable that stores the Adapter install location. By default, Adapter is installed in the /opt/**arcot** directory.

2. Restart the SiteMinder Policy Server.

For SAML Integration

To deploy the properties files for SAML integration:

1. If you plan to install the SAML sample application on the system where AFM is hosted, then *skip* this step. Else, copy the **saml_config.properties**, **samlsampleapp.properties**, and **sampleapps-log4j.properties** from *AFM_HOME*/conf/afm folder to *AFM_HOME*/conf/afm on the system where you plan to deploy the SAML sample applications.
   For information about deploying the SAML sample application, see Deploying the Sample Application WAR Files (see page 93).

2. After deploying the SAML sample applications, restart the application server.

For VPN Integration

If the AFM wizard and AFM are deployed on separate systems, then you must copy the arcotafm.properties file to the AFM_HOME/conf/afm location on the system where AFM is deployed.

Chapter 6: Deploying and Configuring State Manager

This chapter walks you through the process of deploying and configuring the State Manager. It covers the following topics:

- Running Database Scripts (see page 67)
- Copying the JDBC Drivers (see page 68)
- Creating a JNDI Connection (see page 70)
- Deploying State Manager (see page 78)

Important! State Manager is required when you are integrating Adapter with any of the following:

- SAML-based Web portal
- SiteMinder
- SSL VPN that is configured to use the ArcotID OTP on Browser authentication mechanism

You *do not* need to configure State Manager for IPsec VPN integration.

Running Database Scripts

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 MS SQL Server:

   state_manager_installation_dir/dbscripts/mssql

   For MySQL:

   state_manager_installation_dir/dbscripts/mysql

   For Oracle:

   state_manager_installation_dir/dbscripts/oracle

2. Run the **arcot-db-config-for-adapter-statemanager-2.2.9.sql** file on the database.

   This command creates the **ARTSTOKENS** table in your database. This 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 the RiskMinder Server.

Copying the JDBC Drivers

State Manager uses *Java Database Connectivity* (JDBC) to connect to the database. The Adapter installation package is shipped with the JDBC drivers required by State Manager. If you are deploying State Manager on Oracle WebLogic Server, use the JDBC driver that is shipped with the application server. For any other application servers, use the JDBC driver that is shipped with the installation package. To successfully deploy State Manager, you need to copy these drivers to the application server installation directory and create the JNDI connection between the database and State Manager.

Following are the JDBC JAR files that you will need to copy to your application server:

- **For MS SQL Server 2005 and 2008:**
  - If the JDK version of the Application Server is 1.5: sqljdbc.jar
  - If the JDK version of the Application Server is 1.6: sqljdbc4.jar
- **For MySQL:** mysql-connector-java-5.1.22-bin.jar

  Note: You can download the JAR file for MySQL from the Internet.
- **For Oracle:** ojdbc14.jar

The following sub-sections walk you through the steps for copying the JDBC JAR required for your database to one of the following application servers:

- Apache Tomcat (see page 69)
- JBoss (see page 69)
- (For Microsoft SQL Server) Oracle WebLogic (see page 70)

Apache Tomcat

Perform the following steps to copy the JDBC drivers:

1. Navigate to the following directory:

   For MS SQL Server:

   state_manager_installation_dir/adapterStateManager/mssql

   For MySQL:

   state_manager_installation_dir/adapterStateManager/mysql

   For Oracle:

   state_manager_installation_dir/adapterStateManager/oracle

2. Copy the JAR file corresponding to the database that you are using to the following application server installation directory.

   For Apache Tomcat 5.5.x:

   Tomcat_root/common/lib

   For Apache Tomcat 6.x and 7.x:

   Tomcat_root/lib

   Note: *Tomcat_root* refers to the Apache Tomcat installation directory.

3. Restart Apache Tomcat.

JBoss

Perform the following steps to copy JDBC JAR file to JBoss:

1. Copy the JDBC JAR file to the following location on the JBOSS installation directory:

   JBOSS_HOME/server/default/lib

2. Restart the application server.

(For Microsoft SQL Server) Oracle WebLogic

If you are using Microsoft SQL Server, perform the following steps to copy the JDBC JAR file to Oracle WebLogic:

1. Copy the *Database_JAR* file to the following directory:

   JAVA_HOME_used_by_Oracle_WebLogic_instance/jre/lib/ext
2. Log in to WebLogic Administration Console.
3. Navigate to **Deployments**.
4. Enable the **Lock and Edit** option.
5. Click **Install** and navigate to the directory that contains the *Database_JAR* file.
6. Click **Next**.

   The Application Installation Assistant screen opens.
7. Click **Next**.

   The Summary screen opens.
8. Click **Finish**.
9. Activate the changes.
10. Restart the Oracle WebLogic server.

Creating a JNDI Connection

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

- Apache Tomcat (see page 71)
- IBM WebSphere (see page 73)
- JBoss (see page 76)
- Oracle WebLogic (see page 77)

Note: Perform steps in this section to create JNDI connections for the primary database server. If database failover support is needed, then you must also specify the data sources with JNDI names for the secondary database server.

Apache Tomcat (C7_CJNDI_TOMCAT)

To create a JNDI connection in Apache Tomcat:

1. Collect the following database-specific information:
   - JNDI Name

     The JNDI name used by the Arcot components.

     Note: The value you enter in the JNDI Name field must *exactly match* the "Primary JNDI Name" that you have configured in the AFM wizard.
   - User ID

     The database user ID.
   - Password

     The database password.
   - JDBC Driver Class

     The JDBC driver class name. Depending on the database you are using, this value would be one of the following:

     For MS SQL Server:

     com.microsoft.sqlserver.jdbc.SQLServerDriver

     For MySQL:

     com.mysql.jdbc.Driver

     For Oracle:

     oracle.jdbc.driver.OracleDriver
   - JDBC URL

     The JDBC URL for the database server. Depending on the database you are using, this URL would be one of the following:

     For MS SQL Server:

     jdbc:sqlserver://*server*:*port*;databaseName=*database_name*;selectMethod=cursor

     For MySQL:

     jdbc:mysql://*host_name*:*port_number*/*database_name*

     For Oracle:

     URL.1=jdbc:oracle:*thin:@*(*DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=host_name)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=service_name)(SERVER=DEDICATED)))*
2. Take a backup of server.xml file present in the *TOMCAT-HOME*/conf directory.
3. Open the server.xml file present in the *TOMCAT-HOME*/conf directory.

4. Use the information that you collected in Step 1 to add an entry in the following format for defining the data source within the *GlobalNamingResources* tag:

   <Resource name="*datasource-name*" auth="Container" type="javax.sql.DataSource" username="*user-id*" password="*password"* driverClassName="*JDBC-driver-class*" url="*jdbc-url*" maxWait="30000" maxActive="32" maxIdle="4" initialSize="4" timeBetweenEvictionRunsMillis="600000" minEvictableIdleTimeMillis="600000"/>

5. Save and close the server.xml file.

6. Take a backup of the context.xml file present in the *TOMCAT-HOME*/conf directory.

7. Open the context.xml file present in the *TOMCAT-HOME*/conf directory.

8. Use the information that you entered in Step 4 to add an entry in the following format for defining the data source within the Context tag. The data source name that you specify in this step must be the same as the data source name that you specify in Step 4.

   <ResourceLink global="*datasource-name*" name="*datasource-name*" type="javax.sql.DataSource"/>

9. Save and close the context.xml file.

IBM WebSphere

To create a JNDI connection in IBM WebSphere:

1. Log in to WebSphere Administration Console.
2. Click Resources and expand the JDBC node.
3. Click JDBC Providers.

   The JDBC Providers screen opens.
4. In the Preferences section, click New.

   The Create a new JDBC Provider screen opens.
5. Perform the following steps to create a JDBC provider:

   Note: Refer to http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.iseries.doc/info/iseries/ae/tdat_ccrtprov.html for more information on JDBC providers.

   a. If you are using MS SQL Server or Oracle, perform the following steps:

      - Specify the Database Type and Provider Type.
      - Select Connection pool data source from the Implementation Type drop-down list.

   b. If you are using MySQL, perform the following steps:

      - Specify User-Defined as the Database Type.
      - Specify the following as the Implementation Class Name:

        com.mysql.jdbc.jdbc2.optional.MysqlConnectionPoolDataSource

   c. Enter a Name for the JDBC provider. You can also enter a **Description** for the JDBC provider.

   d. Click **Next**.

      The Enter database class path information screen opens.

   e. Enter the absolute path for the JAR file.

   f. Click Next.

      The Summary screen opens.

   g. After reviewing the summary of the information that you have entered, click Finish.
6. Set the CLASSPATH for the JDBC provider that you created in Step 5.

   a. Click Resources and expand the JDBC node.

   b. Click JDBC Providers.

      The JDBC Providers screen opens.

c. Click the JDBC provider that you created in Step 5.

d. Set the Class Path for the JDBC JAR.

e. Click Apply to save the changes.

7. Create a Data Source, as follows:

a. Go to Resources, and then click JDBC.

b. Under JDBC, open Data Sources and click New. Perform the following steps to create a data source:

c. Specify the Data source name.

d. Specify the JNDI name.

Note: The value you enter in the **JNDI name** field must *exactly match* the "Primary JNDI Name" that you have configured in the AFM wizard.

e. Click *Next.*

f. Select an existing JDBC provider created in Step 3.

g. Click Next.

The Enter database specific properties for the data source screen opens.

h. Depending on the database, enter the following information:

- **For MS SQL Server:**

  Specify the Database name, Port number, and Server name.

- **For Oracle**:

  Specify the v**alue** for JDBC URL. This URL would be of the following type:

  jdbc:oracle:thin:@*server*:*port-number*:*sid*

i. Select the **Data store helper class name**. For MySQL, ensure that the data store helper class name is **com.ibm.websphere.rsadapter.GenericDataStoreHelper**.

j. Click **Next**.

The Setup Security aliases screen opens.

k. Click **Next** to view the Summary screen, and then click **Finish**.

8. Click the data source created in Step 7.

9. If you are using MS SQL Server or Oracle, perform the following steps:

a. In the **Related Items** section, click **JAAS - J2C authentication data**.

b. Click **New** to create a new credential.

c. Enter login credentials that are used to connect to the database and save the credential.

d. Click **Apply**, and then click **OK** to save the changes made.

e. Click **Data Sources** and select the data source that you created in Step 7.

f. Under **Security Settings** -> **Component-managed authentication alias**, select the JAAS credential that you created in Step and click **Apply**, and then **OK**.

10. If you are using MySQL, perform the following steps:

    a. Click the **Custom Properties** link.

       A screen showing the existing custom properties opens.

    b. Click New, and enter values for the following properties:

       - databaseName

         Enter a value in the *dbname*?autoReconnect=true format.

       - user
       - password
       - port

         Enter 3306 for MySQL.

       - serverName

    c. Log in again to WebSphere Administration Console.

    d. Go to **Resources**, and then click **JDBC**.

11. Click **Data Sources** and select the check box for the data source you created in Step 7.

12. Click **Test connection** to verify that you have specified the connection correctly.

    Note: This test only checks the connection to the database server, not necessarily the correct definition of the data source. On MySQL, if you find that the connection test fails even though you have specified the correct connection parameters, restart the application server and then retry the connection test.

JBoss

To create a JNDI connection in JBoss:

1. Access the JBOSS AS (Administration Console).
2. In the left pane, click the **Resources**, **Datasources**, **Local Tx DataSource**.

   The Local Tx Datasource screen opens.
3. Click **Add a new resource** button.
4. In the **Select Resource Template** field, select **default (Local Tx Datasource**).
5. Click **Continue**.

   The Add New datasource screen opens.
6. Enter the following information to create a new data source:
   - JNDI Name

     The JNDI name used by the Arcot components.

     Note: The value you enter in the JNDI Name field must *exactly match* the "Primary JNDI Name" that you have configured in the AFM wizard.
   - Username

     The database user name.
   - Password

     The database password.
   - JDBC Driver Class

     The JDBC driver class name. For example, oracle.jdbc.driver.OracleDriver.
   - Connection URL

     The connection URL for the database server. For example, if you are using Oracle driver, then URL would be: jdbc:oracle:thin:*server*:*port-number*:*sid*.
7. Click **Save**.

Oracle WebLogic

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

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

1. Log in to WebLogic Administration Console.
2. Click the Lock & Edit button, if it is not done.
3. Go to Resources, and then click JDBC.
4. Under JDBC, open Data Sources, and click New to create a new data source.

   In case of Oracle WebLogic 11*g*, navigate to Services, then JDBC, and finally to Data Sources.
5. Set the following JNDI and database information:
   a. Specify the name of the data source in the Name field.
   b. Specify the JNDI name in the JNDI Name field.

      Note: The value you enter in the JNDI Name field must exactly match the "Primary JNDI Name" that you have configured in the AFM wizard.
   c. Choose a suitable Database Type, for example Oracle.
   d. Select a suitable Database Driver, for example Oracle Thin Driver.
6. Click Next, retain the default values, and then click Next again.
7. In the Connection Properties page, set the database details. The values mentioned here are for the Oracle database:
   - Database: SID or service name of the DB server
   - Hostname: The IP address or host name of the DB server
   - Port: 1521 or any other port the DB server is running
   - Database User Name
   - Database Password / Confirm Password
8. Click **Test Configuration** to verify that you have specified the correct database parameters.
9. Click **Next** and set the data source target to the preferred WebLogic server instance.
10. Click **Finish** to return to the data source list page.
11. Click **Activate** to enable the data source settings.

Deploying State Manager

Important! If you are integrating Adapter with SAML or SiteMinder, and you have opted to use CA RiskMinder for risk evaluation, then ensure that the RiskMinder Server is started and running.

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

- If you are using MS SQL database with State Manager:

  state_manager_installation_dir/adapterStateManager/mssql

- If you are using MySQL with State Manager:

  state_manager_installation_dir/adapterStateManager/mysql

- If you are using Oracle database with State Manager:

  state_manager_installation_dir/adapterStateManager/oracle

To deploy State Manager, depending on the database you are using, install the arcotsm.war file from one of the preceding locations on your application server. For example, on Apache Tomcat, the location to install the WAR file is:

application_server_home/**webapps**

Apache Tomcat extracts the WAR file and creates a folder named arcotsm under the webapps folder.

Note: Refer to the vendor documentation for instructions on how to deploy on other supported application servers. Also, it is recommended that you use a secured communication channel between all Adapter components. For more information about configuring SSL communication, see Configuring SSL in Apache Tomcat (see page 173).

The following subsections list the additional steps required to deploy State Manager on IBM WebSphere application server.

Applicable Only for IBM WebSphere 6.1

Perform the following steps to deploy WAR file on WebSphere 6.1:

1. Log in to the IBM WebSphere administration console.
2. Navigate to Applications > Install New Application.
3. Based on the location of the WAR file, select either Local file system or Remote file system.
4. In the Full path field, enter the absolute path of the WAR file or click Browse to select the WAR file location.
5. Specify arcotsm as the context root.

6. In the How do you want to install the application section, select the Show me all installation options and parameters option.
7. Click Next.
8. Click Next on the Preparing for the application installation screen.
9. Click Continue on the Application Security Warnings screen.
10. In the Step 1: Select install options screen, select the Precompile JavaServer Pages files option.
11. Click Next.
12. Click Next on the Step 2: Map modules to servers screen.
13. In the Step 3: Provide options to compile JSPs screen, enter the value 15 in JDK Source level column.
14. Follow the onscreen instructions and complete the deployment.

Perform the following steps after you deploy the WAR file:

1. Log in to the IBM WebSphere administration console.
2. Navigate to Applications > Enterprise Applications > WebSphere enterprise applications.
3. Click the WAR file link.
4. Click the Class loading and update detection link.
5. In the Class loader order section, select the Classes loaded with local class loader first option.
6. In the WAR class loader policy section, select the Single class loader for application option.

Applicable Only for IBM WebSphere 7.1

Perform the following steps after you deploy the WAR file:

1. Log in to the IBM WebSphere administration console.
2. Navigate to Applications > Application Types > WebSphere enterprise applications.
3. Click the WAR file link.
4. Click the Class loading and update detection link.
5. In the Class loader order section, select the Classes loaded with local class loader first (parent last) option.
6. In the WAR class loader policy section, select the Single class loader for application option.

Chapter 7: Deploying and Configuring Authentication Flow Manager

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

- Deploying Authentication Flow Manager (see page 82)
- Next Steps (see page 86)

Important! Before deploying and configuring AFM, ensure that AuthMinder is installed, configured, and running.

Deploying Authentication Flow Manager

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

afm_installation_dir/adapterAFM/

To deploy the AFM application, install the arcotafm.war file on your application server. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script. This script is located in the *adapter-install-location* directory.

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

application_server_home/webapps

Apache Tomcat extracts the WAR file and creates a folder named arcotafm under the webapps folder.

Note: Refer to the vendor documentation for deployment instructions on other supported application servers. Bear in mind that you must set the AFM_HOME environment variable *before* you restart the application server.

Depending on the application server that you are using, perform the additional steps described in one of the following sections:

- Applicable Only for JDK 1.5 on Apache Tomcat
- Applicable Only for IBM WebSphere 6.1
- Applicable Only for IBM WebSphere 7.1
- Applicable Only for Oracle WebLogic
- Applicable Only for JBoss 5.1

Applicable Only for JDK 1.5 on Apache Tomcat

Important! The additional configurations given in this section are required *only* when you are integrating Adapter with SAML-based web portal.

Perform the following steps to deploy the JAR files on an Apache Tomcat installation that is using JDK 1.5:

1. Browse to the location where the Adapter installer file is unzipped.
2. Copy the JAR files from the endorsed folder to the location configured for the -Djava.endorsed.dirs system property.
3. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.
4. Restart the application server for the changes to take effect.

Applicable Only for IBM WebSphere 6.1

Perform the following steps to deploy the WAR file on WebSphere 6.1:

1. Log in to the IBM WebSphere administration console.
2. Navigate to Applications > Install New Application.
3. Based on the location of the WAR file, select either Local file system or Remote file system.
4. In the Full path field, enter the absolute path of the WAR file or click Browse to select the WAR file location.
5. Specify arcotsm as the context root.
6. In the How do you want to install the application section, select the Show me all installation options and parameters option.
7. Click Next.
8. Click Next on the Preparing for the application installation screen.
9. Click Continue on the Application Security Warnings screen.
10. In the Step 1: Select install options screen, select the Precompile JavaServer Pages files option.
11. Click Next.
12. Click Next on the Step 2: Map modules to servers screen.
13. In the Step 3: Provide options to compile JSPs screen, enter the value **15** in **JDK Source level** column.
14. Follow the onscreen instructions and complete the deployment.

Perform the following steps after you deploy the WAR file:

1. Log in to the IBM WebSphere administration console.
2. Navigate to Applications > Enterprise Applications > WebSphere enterprise applications.
3. Click the WAR file link.
4. Click the Class loading and update detection link.
5. In the Class loader order section, select the Classes loaded with local class loader first option.
6. In the WAR class loader policy section, select the Single class loader for application option.
7. Use the admin console of the application server to start AFM and then State Manager.

Applicable Only for IBM WebSphere 7.0

Perform the following steps after you deploy the WAR file:

1. Log in to the IBM WebSphere administration console.
2. Navigate to Applications > Application Types > WebSphere enterprise applications.
3. Click the WAR file link.
4. Click the Class loading and update detection link.
5. In the Class loader order section, select the Classes loaded with local class loader first (parent last) option.
6. In the WAR class loader policy section, select the Single class loader for application option.
7. Use the admin console of the application server to start AFM and then State Manager.

Applicable Only for Oracle WebLogic

Important! The additional configurations given in this section are required *only* when you are integrating Adapter with SAML-based web portal.

Perform the following steps:

1. Stop the WebLogic Server.
2. Create a directory named endorsed, if it does not already exist, in the *JAVA_HOME*/jre/lib directory.
3. If there is an existing *JAVA_HOME*/jre/lib/endorsed directory, take a backup of the following JAR files and then delete them from the *JAVA_HOME*/jre/lib/endorsed directory:
   - resolver
   - serializer
   - xalan
   - xercesImpl
   - xml-apis
4. Copy the JAR files that are available in the endorsed directory of the Adapter package to the *JAVA_HOME*/jre/lib/endorsed directory.
5. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.
6. Start the WebLogic server.

Applicable Only for JBoss 5.1

Important! The additional configurations given in this section are required *only* when you are integrating Adapter with SAML-based web portal.

Perform the following steps:

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

   JBOSS_Install_Home/lib /endorsed
3. If the following files are present in the *JBOSS_HOME*/lib /endorsed directory, take a backup of the files and then delete them from *JBOSS_HOME*/lib /endorsed.
   - resolver
   - serializer
   - xalan
   - xercesImpl
   - xml-apis
4. Copy the JAR files available in the endorsed directory of the Adapter package *to* the following location:

   JBOSS_HOME/lib/endorsed
5. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.
6. Start the JBoss application server.

Next Steps

Based on your integration type, proceed with the configuration steps that are discussed in this section.

- For SiteMinder Integration
  a. Complete the Authentication Shim, FCC pages, and SiteMinder configurations, as discussed later in this guide.
  b. Verify the integration as discussed in Verifying SiteMinder Integration (see page 105).
- For SAML Integration
  a. Deploy and configure the SAML sample applications, as discussed in Deploying and Configuring SAML Sample Applications (see page 93).
  b. Verify the integration, as discussed in Verifying SAML Integration (see page 105).
- For Cisco IPSec VPN Integration

  Perform the post-installation configuration tasks described in the *CA Adapter for Cisco IPSec VPN Configuration Guide*.
- For Juniper SSL VPN Integration

  Perform the post-installation configuration tasks described in the *CA Adapter for Juniper SSL VPN Configuration Guide*.

Chapter 8: Configuring Authentication Shim and FCC Pages

This chapter describes how to configure the Form Credential Collector (FCC) pages and Authentication Shim. It covers the following topics:

- Deploying the FCC Pages (see page 87)
- Deploying Authentication Shim (see page 87)

Deploying the FCC Pages

To deploy the FCC pages, copy the complete FCC directory available at the following location to the appropriate location on the Server where the Web Agent is installed.

installation_dir/adapterSiteMinder/fcc/

In addition to copying the complete FCC directory, you must also create a virtual directory in the Web Server that points to the FCC directory that you copied.

Deploying Authentication Shim

The files required to deploy Authentication Shim are available at the following location on the SiteMinder Policy Server system:

auth_shim_installation_dir/adapterSiteMinder/lib/

To deploy the Authentication Shim:

1. Ensure that the Authentication Shim library and the log library files are available in the system LD_LIBRARY_PATH system variable by doing one of the following:
   - Copying the ArcotSiteMinderAdapter.so and ArcotLog2FileSC.so files, available in the *auth_shim_installation_dir*/adapterSiteMinder/lib directory

     to the lib directory of the SiteMinder Policy Server.
   - Including the *auth_shim_installation_dir*/adapterSiteMinder/lib directory in the LD_LIBRARY_PATH variable.
2. Restart the SiteMinder Policy Server.

Chapter 9: Configuring CA SiteMinder Policy Server

To configure SiteMinder Policy Server to integrate with Adapter, perform the following steps (on the system hosting SiteMinder Policy Server). The steps documented here are for SiteMinder Policy Server version 12. If you are using a different version of the SiteMinder Policy Server, refer to the relevant SiteMinder Policy Server documentation.

1. Create a new Authentication Scheme in the SiteMinder Policy Server administrative interface, as follows:

    a. Open SiteMinder Policy Server Administrative User Interface, click the Infrastructure tab, click Authentication, and then click Authentication Scheme.

    b. Click Create Authentication Scheme.

    c. In the Create Authentication Scheme screen, select Create a new object of type Authentication Scheme, and click OK.

    d. In the General section of the Create Authentication Scheme screen, do the following:

    - Specify a name and description for the new authentication scheme in the Name and Description fields respectively.
    - Select Custom Template from the Authentication Scheme Type drop-down list.
    - Specify a protection level. The protection level is enforced during single sign-on when the user tries to access resources protected by different authentication schemes.
    - Some authentication scheme types support Password Policies, while others do not. Select the Password Policies enabled for this Authentication Scheme check box, if you want the authentication scheme to support password policies.

e. In the Scheme Setup section of the Create Authentication Scheme screen, do the following:

- Enter the Adapter library file name as ArcotSiteMinderAdapter in the Library field.
- Enter the name of the configured workflow in the Parameter field.

Important! The value you enter in the Parameter field is *case-sensitive* and it must exactly match the "AFM Profile Name" that you have configured in the AFM wizard.

Note: You must append the profile name with the *installation_directory* 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 profile name is OnePage, then the Parameter field must be specified as OnePage,/opt/arcot. In addition, SectionName *must* match the AFM Profile Name that you specified using the Wizard.

f. Click Submit to create the authentication scheme.

2. Any realm that you wish to protect with Arcot authentication 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 Adapter, set the parameters from the following table in the SiteMinder Agent Configuration Object Dialog screen.

Parameter	**Value**
CssChecking	Yes
FCCCompatMode	Yes
AgentName	Name of the agent.
LogFileName	Name of the Web Agent log file. This is not a mandatory setting, but can be used for debugging.
DefaultAgentName	Name of the default Web Agent.
DefaultPassword	Web Agent password.
LogFileSize	Size of the Web Agent log file.
Logfile	Yes
RequireCookies	Yes
TraceConfigFile	Name of the trace configuration file. This is not a mandatory setting, but can be used for debugging.
TraceFile	Yes
TraceFileName	Name of the trace file.

Parameter	Value
TraceFileSize	Size of the trace file.

Chapter 10: Deploying and Configuring SAML Sample Applications

SAML sample applications can be used to verify if Adapter was successfully installed and configured for SAML integration. In addition, it demonstrates:

- The typical authentication workflows supported by Adapter
- Integration of your application with Adapter

Important! Sample application must not be used in production deployments. The sample application is provided to demonstrate the AFM SAML workflows.

This chapter covers the following topics:

- Deploying the Sample Application WAR Files (see page 93)
- Verifying the Sample Application Deployment (see page 97)
- Configuring Sample Application (see page 97)

Chapter 11: Deploying the Sample Application WAR Files

The Adapter installation package includes the following SAML sample applications:

- **samlsampleapp.war**: The main sample application.
- **bankapp.war**: The sample bank application.
- **insuranceapp.war**: The sample insurance application.

Using these modules, you can test the authentication workflows available in the SAML integration. To deploy sample application:

1. Navigate to the following location:

   saml_sample_app_installation_dir/sampleApplications

2. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script. This script is located in the *adapter-install-location* directory.

3. Copy the samlsampleapp.war, bankapp.war, and insuranceapp.war files to your application server. For example on Apache Tomcat, the location to copy the WAR file is:

   application_server_home/**webapps**

   Apache Tomcat automatically deploys the WAR files and creates the following folders under the webapps folder:

   - samlsampleapp
   - bankapp
   - insuranceapp

Note: Refer to the vendor documentation for deployment instructions on other supported application servers. Bear in mind that you must set the $AFM_HOME environment variable *before* you restart the application server.

1. (**Applicable Only for JDK 1.5 on Apache Tomcat**) Perform the following steps to deploy the JAR files on an Apache Tomcat installation that is using JDK 1.5:

   a. Browse to the location where the Adapter installer file is unzipped.

   b. Copy the JAR files from the endorsed folder to the location configured for the -Djava.endorsed.dirs system property.

   c. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.

   d. Restart the application server for the changes to take effect.

2. (**Applicable Only for IBM WebSphere 6.1**) Perform the following steps to deploy WAR file on WebSphere 6.1:

   a. Log in to the IBM WebSphere administration console.

   b. Navigate to **Applications** > **Install New Application**.

   c. In the **How do you want to install the application** section, select the **Show me all installation options and parameters** option.

d. Click **Next**.

e. Click **Next** on the Preparing for the application installation screen.

f. Click **Continue** on the Application Security Warnings screen.

g. In the Step 1: Select install options screen, select the **Precompile JavaServer Pages files** option.

h. Click **Next**.

i. Click **Next** on the Step 2: Map modules to servers screen.

j. In the Step 3: Provide options to compile JSPs screen, enter the value **15** in **JDK Source level** column.

k. Follow the on-screen instructions and complete the deployment.

3. (**Applicable Only for IBM WebSphere 6.1**) Perform the following steps after you deploy the WAR file:

   a. Log in to the IBM WebSphere administration console.

   b. Navigate to **Applications** > **Enterprise Applications** > **WebSphere enterprise applications**.

   c. Click the WAR file link.

   d. Click the **Class loading and update detection** link.

   e. In the **Class loader order** section, select the **Classes loaded with local class loader first** option.

   f. In the WAR class loader policy section, select the **Single class loader for application** option.

   g. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.

   h. Restart IBM WebSphere.

4. (**Applicable Only for IBM WebSphere 7.0**) Perform the following steps after you deploy the WAR file:

   a. Log in to the IBM WebSphere administration console.

   b. Navigate to **Applications** > **Enterprise Applications** > **WebSphere enterprise applications**.

   c. Click the WAR file link.

   d. Click the **Class loading and update detection** link.

   e. In the **Class loader order** section, select the **Classes loaded with local class loader first (parent last)** option.

   f. In the WAR class loader policy section, select the **Single class loader for application** option.

   g. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.

h. Restart IBM WebSphere.

5. (**Applicable only for Oracle WebLogic**) Perform the following steps:

   a. Stop the WebLogic Server.

   b. Create a directory named endorsed, if it does not already exist, in the *JAVA_HOME*/jre/lib directory.

   c. If there is an existing *JAVA_HOME*/jre/lib/endorsed directory, take a backup of the following JAR files and then delete them from the *JAVA_HOME*/jre/lib/endorsed directory:

      - resolver
      - serializer
      - xalan
      - xercesImpl
      - xml-apis

   d. Copy the JAR files that are available in the endorsed directory of the Adapter package to the *JAVA_HOME*/jre/lib/endorsed directory.

   e. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.

   f. Start the WebLogic server.

6. (**Applicable Only for JBoss 5.1**) Perform the following steps:

   a. Stop the JBoss application server.

   b. Navigate to the following location:

      JBOSS_Install_Home/lib /endorsed

   c. If the following files are present in the *JBOSS_HOME*/lib /endorsed directory, take a backup of the files and then delete them from *JBOSS_HOME*/lib /endorsed.

   - resolver
   - serializer
   - xalan
   - xercesImpl
   - xml-apis

   a. Copy the JAR files available in the endorsed directory of the Adapter package *to* the following location:

      JBOSS_HOME/lib/endorsed

   b. To set the $AFM_HOME environment variable on the system, run the afmenv.sh script from the *adapter-install-location* directory.

   c. Start the JBoss application server.

Chapter 12: Verifying the Sample Application Deployment

The webapps folder must now contain the following folders:

- samlsampleapp
- bankapp
- insuranceapp

You can access the following URL from the end-user's system:

http[s]://host_name:port_number/samlsampleapp/

Replace *host_name* and *port_number* with the host name and port of the system where you have deployed sample application. The main page of sample application opens.

If you see the welcome page of sample application, it indicates that you have successfully deployed SAML sample application.

Chapter 13: Configuring Sample Application

Important! Ensure that the system time of SAML sample application and the system where AFM is deployed is in sync. If the time is not in sync, then SAML sample application will throw an authentication failure error.

After deploying sample application, you need to configure it before you can test it. To configure sample application, perform the following tasks:

- Performing Basic AFM Configurations Using Sample Application (see page 97)
- (Optional) Configuring Custom Certificates in Sample Application (see page 98)

Chapter 14: Performing Basic AFM Configurations Using Sample Application

Perform the following steps to configure SAML sample application:

1. From the end-user's system, access sample application in a Web browser window. The default URL for sample application is:

   http[s]://host_name:port_number/samlsampleapp/

   The main page of sample application opens.

2. Click **Setup**.

   The AFM setup screen opens.

3. On the AFM setup page, provide the following information:

   a. **Arcot AFM Protocol**: Select a protocol for establishing the communication channel with the application server hosting AFM.

      Note: If you are using ArcotID PKI Flash client, then you must select the **https** protocol. For more information about ArcotID PKI Flash client, see the *ArcotID Client Reference Guide* available with the CA AuthMinder documentation.

   b. **Arcot AFM Host**: Specify the FQDN or IP address of the application server hosting AFM.

   c. **Arcot AFM Port**: Specify the port at which the application server hosting AFM is available.

   d. **Flow type**: Select an AFM profile from the list of available profiles that is displayed in the drop-down list. These profiles would have been created at the time of configuring Adapter. For information about creating AFM profiles, see Performing Adapter Configuration Using the Wizard (see page 47).

4. Click **Submit**.

   The "Setup Successful" message opens.

Chapter 15: (Optional) Configuring Custom Certificates in Sample Application

SAML sample application can be configured to use a different set of certificates instead of bundled sample certificates. To configure sample application to use different certificates:

1. Navigate to the location where you have deployed SAML sample application. For example, navigate to the following location:

   AFM_HOME/conf/afm

2. Open the samlsampleapp.properties file in a text editor.
3. Configure the properties, as described in the following table:

Property	Description
SamlSigningCertPath	Specify the complete path of the X.509 certificate that will be used to verify the SAML response. The corresponding key store must be used in AFM for signing the SAML response. **Note:** The certificate must be in .DER format.
SamlSigningPrivateKeyPath	Specify the complete path of the key store file that is used to sign the SAML request. **Note:** Ensure that the public-private key-pair is generated using "RSA" as the key algorithm and "SHA1withRSA" as the signing algorithm.
SamlSigningKeyStoreAlias	Specify an alias of the private key and certificate stored in the key store.
SamlSigningJKSPassword	Specify the password for the key store.

4. Save and close the samlsampleapp.properties file.
5. Restart the application server.

Chapter 16: Configuring the Service Provider's Application

This chapter provides an overview of how to integrate your SAML enabled applications with AFM. The JSPs explained in this chapter are available in the *application_server_home*/webapps/arcotafm/ directory.

- **master.jsp**: This JSP provides pointers to the JSPs for the individual workflows that are configured in the JSPs listed in the "Authentication Flow Manager" (see page 14) section.

  To integrate your application with AFM, you need to configure your application to send authentication or user migration request to the master.jsp file. You can configure your application to send a request in any one of the following ways:

  a. **Service Provider Initiated Workflow**: In this approach, the Service Provider's application sends the authentication request to AFM. In this approach, the parameters described in the following table must be passed in the request.

Parameter	Description
SigAlg	The algorithm used by your application for signing the request.
Signature	The signature of the parameters as explained in the SAML Protocol.
SAMLRequest	Base64 encoded SAML request.
RelayState	This is an opaque reference to the state on the Service Provider's side. This is an *optional* parameter.
Profile	This is the AFM profile created from Wizard. This defines the primary and secondary authentication mechanisms and other related configurations.
Processreq	This is used by AFM.

  b. **Identity Provider Initiated Workflow**: In this workflow the user can either directly hit the AFM URL or the Service Provider can redirect the user's authentication request to AFM with the parameters described in the following table:

Parameter	Description
Profile	This is the AFM profile created from Wizard. This defines the primary and secondary authentication mechanism and other related configurations.
Processreq	This used by AFM.

If you are using the second approach (Step), then you need to configure the AssertionConsumerServiceURL property in the saml_config.properties file. This property specifies the URL where the SAML response (generated after authentication) has to be posted back.

After user's authentication request is processed, AFM generates a SAML response and sends it back to the Service Provider's application. The Service Provider's application needs to verify this response. You may need to configure the following properties based on your SAML Service Provider implementation:

- SignSamlAssertionOnly: Specify whether the complete SAML response or only the assertion part of the response needs to be signed.
- CanonicalizationMethod: Specify the canonicalization method that is applied to the SAML response before signing it.

- **settings.jsp**: This JSP is used to enable end users to update their credentials. The workflow defined in this JSP updates the credentials of the user. When you integrate this JSP in your application, ensure that a link to this JSP is displayed to the end user only after successful authentication. Use the following format for the URL that leads to this JSP:

  /arcotafm/settings.jsp?profile=profile-name

  This URL must also include a signed SAML request in the query parameter.

- **masterEnrollment.jsp**: The workflow defined in this JSP enrolls the user for the configured AuthMinder credentials. This is done after authenticating the user with LDAP, OTP, or both, depending on the configuration. If a profile has been configured in the AFM wizard, then to enroll the user for the credentials configured in the profile, ensure that a request parameter is sent from your application to this JSP in the following format:

  arcotafm/masterEnrollment.jsp?profile=profile-name

Chapter 17: Verifying Adapter Integration

This chapter covers the following topics:

- Verifying the State Manager Configuration (see page 103)
- Verifying the AFM Configuration (see page 104)
- Verifying the Authentication Shim Configuration (see page 104)
- Verifying SiteMinder Integration (see page 105)
- Verifying SAML Integration (see page 105)

Verifying the State Manager Configuration

To test the State Manager configuration:

1. Run the afmenv.sh script. This script is located in the *adapter-install-location* directory. It sets the $AFM_HOME environment variable.
2. Restart the application server where State Manager is installed.
3. Access State Manager by using the following URL:

   http[s]://host_name:port_number/arcotsm/index.jsp

   Replace *host_name* and *port_number* with the host name and port of the system where you have deployed State Manager. The State Manager Operations page opens.
4. Click **Create token**.

   A sample token is created.
5. Open the **arcotsm.log** file, which is available on the system where State Manager is hosted. The default location of this log file is:

   AFM_HOME/logs
6. Search for the following lines in the log file, which indicate that State Manager is configured successfully:

   Servlet com.arcot.integrations.toksvr.server.TokenCreator starting up

   ...

   Servlet com.arcot.integrations.toksvr.server.TokenRemover starting up

   ...

   Servlet com.arcot.integrations.toksvr.server.TokenReader starting up

Verifying the AFM Configuration

To test the AFM configuration:

Note: If AFM and State Manager are deployed on the same application server and if State Manager is started after AFM, then an error message might get recorded in the log. You can ignore this error because it does not affect the functioning of AFM or State Manager.

1. Open the arcotafm.log file, which is available on the system hosting the AFM application. The default location of this log file is:

   AFM_HOME/logs

2. Search for the following lines in the log file, which indicate that AFM is configured successfully.

   WebFort 7.1.01 Authentication SDK initialized successfully.

   WebFort 7.1.01 Issuance SDK initialized successfully.

Verifying the Authentication Shim Configuration

To test the Authentication Shim configuration:

1. Open the arcotadaptershim.log log file available in the *auth_shim_installation_dir*/logs directory.

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

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

   Logger initialized

   STARTING [Authentication Shim 2.2.9.0]

Verifying SiteMinder Integration

To test the SiteMinder integration:

Note: For testing purposes, the protected resource in SiteMinder is configured to use the ArcotID PKI workflow. If you have configured the protected resource for any other authentication mechanism, then you will not see the same FCC pages described in this section.

1. Restart the application server where AFM is installed.
2. Restart SiteMinder Policy Server and Web Agent services.
3. From the end-user's system, access the protected resource that you configured in SiteMinder.

   The FCC page.
4. Enter the user name existing in the User Directory configured in SiteMinder.
5. Click **Continue**.

   If the user is not enrolled for ArcotID PKI authentication, then the AFM User Enrollment screen opens.

   If you see the AFM page, it indicates that you have successfully configured Adapter with SiteMinder.

Verifying SAML Integration

To test the SAML integration by using SAML sample application:

1. From the end-user's system, launch a new instance of the Web browser and access the main page of sample application by using the following URL:

   http[s]://host_name:port_number/samlsampleapp/

   Replace *host_name* and *port_number* with the host name and port of the system where you have deployed sample application.

   The main page of sample application opens.
2. Click the **Banking Account** link.

   The authentication page that opens depends on the authentication workflow that you have configured.

   If you see the AFM page, it indicates that you have successfully configured Adapter with SAML sample application.

Chapter 18: Uninstalling Adapter

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

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

- Dropping the Adapter Schema (see page 107)
- Uninstalling Adapter (see page 108)
- Post-Uninstallation Steps (see page 109)

Dropping the Adapter Schema

Note: If for some reason, you need to retain the database, then *do not* proceed with the instructions in this section. You can start with the uninstallation instructions in Uninstalling Adapter (see page 108).

Perform the following tasks to uninstall the Adapter database schema:

1. Based on the database that you are using, navigate to one of the following subdirectories:

   For MS SQL Server:

   state_manager_installation_dir/dbscripts/**mssql**/

   For MySQL:

   state_manager_installation_dir/dbscripts/**mysql**/

   For Oracle:

   state_manager_installation_dir/dbscripts/**oracle**/

2. Run the **drop-adapter-statemanager-2.2.9.sql** script.

Uninstalling Adapter

To uninstall Adapter, you must remove the components installed during the installation process. Perform the following steps on the systems where you have installed Adapter components:

1. Navigate to the following directory:
   installation_dir/Uninstall_Arcot Adapter 2.2.9/
2. Run the installer using the following command:
   prompt>**Uninstall_Arcot_Adapter_2.2.9**

   The Uninstall Options screen opens.
3. Enter the enter corresponding to the type of uninstallation you want to perform. The options are:
   - **1-Completely remove all components... :** Select this option if you want to uninstall *all* components of Adapter from the current system.
   - **2-Choose specific components... :** Select this option if you want to uninstall only *selected* components of 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 opens.
5. (For Uninstalling Specific Components Only) This screen displays the Adapter components that are installed on the current system. Enter the number of the components (separated by a comma) that you want to uninstall from the current system.
6. Press **Enter**. The Choose Backup Location screen opens.
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 Adapter components.
8. The Uninstall Complete screen opens at the end of successful uninstallation and the system returns to the command prompt.

Post-Uninstallation Steps

You need to perform the following post-uninstallation steps to ensure that all Adapter components are removed:

1. If the installation directory (*installation_dir*) exists, delete it.

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

2. Uninstall the following WAR files from the appropriate subdirectory in the application server installation directory. Refer to the application server vendor documentation for detailed information on uninstalling the WAR files.

   - arcotafm.war: Authentication Flow Manager
   - arcotsm.war: State Manager
   - ArcotAFMWizard.war: Arcot Configuration Wizard application
   - Sample application WAR files:
     - samlsampleapp.war: The main sample application.
     - bankapp.war: The sample bank application.
     - insuranceapp.war: The sample insurance application.

   Note: You have to locate these files on the system where you have deployed the particular component.

Appendix A: Adapter File System Structure

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

Important! In addition to the directories and files discussed in this table, you will also see the adapterkey and arcotkey 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.

Component	Location	Files
Authentication Flow Manager	*installation_dir*/adapterAFM	Contains the WAR files and the following subdirectory: ■ certs Stores the keystore and truststore files that AFM requires. **Note:** These key store and trust store files are bundled with the package for testing purposes only. You can use these files to enable two-way SSL communication between AFM and State Manager.
	installation_dir/docs	Contains the AFM Java documents.

Component	Location	Files
State Manager	*installation_dir*/ adapterStateManager	Contains the following subdirectories: ■ certs Stores the keystore and truststore files that State Manager requires. **Note:** These key store and trust store files are bundled with the package for testing purposes only. You can use these files to enable two-way SSL communication between State Manager, Authentication Shim, and AFM. ■ mssql Store the State Manager's WAR file and the JDBC drivers for MS SQL Server. ■ mysql Store the State Manager's WAR file. ■ oracle Store the State Manager's WAR file and the JDBC driver for the Oracle Database server.

Component	Location	Files
	installation_dir/dbscripts	Contains the SQL scripts required to create the State Manager schema in the supported database. Contains the following subdirectories: ■ mssql Stores the SQL scripts for creating and dropping database schema in MS SQL Server. ■ mysql Stores the SQL scripts for creating and dropping database schema in MySQL. ■ oracle Stores the SQL scripts for creating and dropping database schema in the Oracle Database server.
AFM Wizard	*installation_dir*/AFMWizard	Contains the ArcotAFMWizard.war file that AFM Wizard requires.

Component	Location	Files
Authentication Shim *(applicable for SiteMinder integration)*	*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 purposes only. You can use these files to enable two-way SSL communication between Authentication Shim and State Manager.

Component	Location	Files
	installation_dir/ adapterSiteMinder/lib	Contains the following files: ■ ArcotLog2FileSC.so: Log library file ■ ArcotSiteMinderAdapter.so: Authentication Shim library file
	installation_dir/ conf	Contains adaptershim.ini that specifies the Authentication Shim configuration parameters.

Component	Location	Files
FCC Pages *(applicable for SiteMinder integration)*	*installation_dir*/ adapterSiteMinder/ fcc	Contains the FCC pages and the following subdirectories: ■ css — Stores a style sheet file called arcot-enrollment.css. ■ fonts — Stores the fonts used by the FCC pages. ■ images — Store the Arcot logo and other image files used by the FCC pages. ■ js — Stores a JavaScript file called ArcotAdapterIntegration.js. The fcc directory contains the following files: ■ shim.fcc — This page accepts the username and LDAP password as input for authenticating the user. This FCC page is used in One-Page login scenarios. ■ shim2.fcc — This page accepts the username, which is used for further processing.

Component	Location	Files
		■ 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 credentials and exceeds the maximum number of login attempts that SiteMinder allows.
Sample Applications	*installation_dir*/sample Applications	Contains the following sample application WAR files: ■ bankapp.war ■ insuranceapp.war ■ samlsampleapp.war ■ customapp.war
Common Files and Directories	*installation_dir*/ ext-license	Contains the third-party software licenses used by Adapter.
	installation_dir/ logs	Contains the log files. It also contains the following subdirectory: ■ backup Stores the rolled over log files of Authenticatio n Shim.

Component	Location	Files
	installation_dir/ Uninstall Arcot Adapter 2.2.9	Contains the files required for uninstalling Adapter.

Appendix B: Configuration Files and Options

This appendix discusses the configuration files that Adapter uses and the parameters that you can configure in these files. The following configuration files are available in Adapter:

- State Manager Properties File (see page 119)
- AFM Properties File (see page 124)
- SAML Properties File (see page 146)
- Authentication Shim Properties File (see page 150)

Note: When updating any of the configuration files, ensure that you uncomment the parameters that you want to configure.

State Manager Properties File

To manually configure the State Manager properties, perform the following steps:

1. Navigate to the following directory on the system where you have installed State Manager:

   AFM_HOME/conf/afm/

2. Open the arcotsm.properties file in a text editor.

   The properties file contains the RiskMinder parameters, as described in the following table.

Parameter	Required/ Optional	Used By	Description
RiskFortHOST.1 RiskFortHOST.2	Required Optional	SiteMinder	Specify the IP address or the *Fully Qualified Distinguished Name* (FQDN) of RiskMinder Server.
RiskFortPORT.1 RiskFortPORT.2	Required Optional	SiteMinder	Specify the port where RiskMinder Server is listening to the incoming requests. Default value: **7680**

Parameter	Required/ Optional	Used By	Description
RiskFortTRANSPORT_TYPE	Optional	SiteMinder	Specify the protocol for RiskMinder Server. **Note:** It is recommended that the communication between State Manager and RiskMinder be over SSL. Refer to the CA RiskMinder Installation and Deployment Guide for more information on how to configure RiskMinder for SSL. Default value: **TCP**
RiskFortCA_CERT_FILE	Optional, *Required only if* RiskFortTRANSPORT_TYPE=SSL	SiteMinder	Specify the *complete path* of the *certification authority (*CA) certificate file for RiskMinder Server. The file *must* be in.PEM format.
RiskFortCLIENT_P12_FILE	Optional, *Required only if* RiskFortTRANSPORT_TYPE=SSL	SiteMinder	Specify the path of the PKCS 12 file that contains the key and certificate of the client that communicates with RiskMinder Server. This would establish two-way SSL between the RiskMinder client and server.
RiskFortCLIENT_P12_PASSWORD	Optional, *Required only if* RiskFortTRANSPORT_TYPE=SSL	SiteMinder	Specify the password for the PKCS 12 file specified in the RiskFortCLIENT_P12_FILE parameter.
RiskFortCONNECTION_TIMEOUT	Optional	SiteMinder	Specify the time (in milliseconds) before RiskMinder Server is considered unreachable. Default value: **30000** (30 seconds)
RiskFortREAD_TIMEOUT	Optional	SiteMinder	Specify the maximum time (in milliseconds) allowed for a response from RiskMinder Server. Default value: **30000** (30 seconds)

Parameter	Required/ Optional	Used By	Description
RiskFortCONNECTION_RETRIES	Optional	SiteMinder	Specify the maximum number of retries allowed to connect to the RiskMinder Server. Default value: **3**
RiskFortUSE_CONNECTION_POOLING	Optional	SiteMinder	Specify whether the connection pooling with RiskMinder Server is enabled or disabled. Possible values are: ■ **1**: Enabled ■ **0**: Disabled Default value: **1**
RiskFortMAX_ACTIVE	Optional	SiteMinder	Specify the number of maximum connections that can exist between State Manager and RiskMinder Server. The number of connections should not exceed this value. Default value: **32**
RiskFortTIME_BETWEEN_CONNECTION_EVICTION	Optional	SiteMinder	Specify the time (in milliseconds) after which the connection eviction thread will be executed to check and delete any idle RiskMinder Server connection. Default value: **900000** (90 seconds)
RiskFortIDLE_TIME_OF_CONNECTION	Optional	SiteMinder	Specify the time (in milliseconds) after which an idle RiskMinder Server connection will be closed. Default value: **1800000** (3 minutes)
RiskFortWHEN_EXHAUSTED_ACTION	Optional	SiteMinder	Specify the behavior when the maximum number of supported connections have exhausted. Default value: **BLOCK**

The following table describes the token-related parameters:

Parameter	Required/ Optional	Used By	Description
TokenMaxInactivitySeconds	Optional	■ SAML ■ SiteMinder	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: **900** (15 minutes)
TokenMaxLifetimeSeconds	Optional	■ SAML ■ SiteMinder	Specify the maximum amount of time (in seconds) for which the token is accessible after it is generated. Default value: **900** (15 minutes)
TokenCleanupIntervalSeconds	Optional	■ SAML ■ SiteMinder	Specify the frequency (in seconds) at which the expired tokens are checked and deleted from the database. Default value: **30**
TSMClass	Optional	■ SAML ■ SiteMinder	Specify the class implementing the type of storage mechanism to be used for State Manager. By default, State Manager uses a JDBC database. Default value: **com.arcot.integrations.toksvr.server.tsmimpl.iBatisTSMImpl**

The following table describes the database connectivity parameters:

Parameter	Required/ Optional	Used By	Description
DbType	Required	■ SAML ■ SiteMinder	Specify the type of database applicable to all database connections. Set the value of this parameter to mssqlserver, mysql, or oracle.
AutoRevert	Optional	■ SAML ■ SiteMinder	Specify 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**

Parameter	Required/ Optional	Used By	Description
AppServerConnectionPoolName.n	Required	■ SAML ■ SiteMinder	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 must be created in the containing application server, and sufficient privileges must be given to State Manager for it to use the connection pool. For example, configure this property in Apache Tomcat, as shown: AppServerConnectionPoolName.1= java:comp/env/jdbc/ArcotStateManagerDataSource1 For other application servers, specify only the JNDI name. For example: AppServerConnectionPoolName.1= jdbc/ArcotStateManagerDataSource1 If Application Server connection pool is not required, then leave this configuration empty.

Note: To enforce secure communication between State Manager and other components, ensure that the parameter RequireSecureConnection is set to true, which is also the default value.

State Manager Log File

To configure the log file for State Manager, perform the following steps:

1. Navigate to the following directory on the system where you have installed State Manager:

   AFM_HOME/conf/afm/

2. Open the arcotsm-log4j.properties file in a text editor, and set the log information as described in the following table:

Parameter	Description
log4j.appender.smlog.File	Specify the log file name and the location where the State Manager log files must be created. By default, on Apache Tomcat, the State Manager log file name is arcotsm.log and it is created in the *AFM_HOME*/**logs** directory.

AFM Properties File

To manually configure the AFM properties, perform the following steps:

1. Navigate to the following directory on the system where you have installed AFM:

   AFM_HOME/conf/afm/

2. Open the arcotafm.properties file in a text editor.

   The following table describes the State Manager configuration parameters in this properties file:

Parameter	Required / Optional	Used By	Description
Most Used State Manager Parameters			
ArcotSMHostname	Required	■ SAML ■ SiteMinder	Specify the *Fully Qualified Distinguished Name* (FQDN) or IP address of State Manager.
ArcotSMPort	Required	■ SAML ■ SiteMinder	Specify the port of the application server where State Manager is deployed.
ArcotSMBaseURL	Optional	■ SAML ■ SiteMinder	Specify the URL where State Manager is available. Default value: **arcotsm/servlet**
ArcotSMSecureConnection	Optional	■ SAML ■ SiteMinder	Specify whether AFM communicates with State Manager in a secure mode over SSL. Possible values are: ■ true ■ false Default value: **true**

Parameter	Required / Optional	Used By	Description
ArcotSMTrustStore	Optional	■ SAML ■ SiteMinder	Specify the path where the root SSL certificate of State Manager is present. This parameter is valid if ArcotSMSecureConnection is set to true. Default value: **/certs/tsclient.truststore** **Note**: This setting is ignored if the JRE parameters javax.net.ssl.trustStore and javax.net.ssl.trustStorePassword are set.
ArcotSMTrustStore Password	Optional (Required, if ArcotSMTrustStore is provided.)	■ SAML ■ SiteMinder	Specify the password of the truststore. This parameter is valid if the ArcotSMTrustStore path is provided. Default value: **123456**
ArcotSMKeyStore	Optional	■ SAML ■ SiteMinder	Specify the path of the client SSL keystore. Default value: **/certs/tsclient.keystore** This setting is ignored if the JRE parameters javax.net.ssl.keyStore and javax.net.ssl.keyStorePassword are set.
ArcotSMKeyStore Password	Optional (Required, if ArcotSMKeyStore is provided.)	■ SAML ■ SiteMinder	Specify the password of the keystore. Default value: **123456**

Parameter	Required / Optional	Used By	Description
Least Used State Manager Parameters			
ArcotAFMLandingURL	Optional	■ SiteMinder	This parameter is used by Authentication Shim or other components that redirect the user's authentication request to AFM to verify whether or not the user's request was processed with the redirected URL. Specify this parameter only if the application server does not map the URL to the same value as Authentication Shim that is used for redirection. Default value: URL of the Controller JSP that receives HTTPRequest.
ArcotSMConnTimeoutMS	Optional	■ SAML ■ SiteMinder	Specify the time (in milliseconds) before State Manager is considered unreachable and the attempt is aborted. Default value: **15000** (15 seconds)
ArcotSMReadTimeoutMS	Optional	■ SAML ■ SiteMinder	Specify the maximum time (in milliseconds) for which AFM must wait for a response from State Manager. **Note:** Do *not* set this parameter to **0** as the client will wait for a response indefinitely. Default value: **30000** (30 seconds)
ArcotSMMaxRetries	Optional	■ SAML ■ SiteMinder	Specify the maximum number of retries allowed to connect to State Manager. Default value: **0** (no retries)

Parameter	Required / Optional	Used By	Description
ArcotSMTestConnAtStartup	Optional	■ SAML ■ SiteMinder	Specify whether a test token must be created when the Web application starts. **Note:** If you are using JRE 1.4.2.x and AFM starts before State Manager, then AFM cannot time-out the connection, and cannot start up. Possible values are: ■ true ■ false Set this to **false** if AFM and State Manager are deployed on the same application server, because the application server may hang if the test is run before State Manager is initialized. Default value: **true**

The following table describes the AuthMinder Server's authentication and issuance-related parameters:

Parameter	Required/ Optional	Used By	Description
Most Used AuthMinder Server Authentication Parameters			

Parameter	Required/ Optional	Used By	Description
WebFortauthentication.host.1 WebFortauthentication.host.2	Optional, Required only if CA AuthMinder is used.	■ SAML ■ SiteMinder ■ VPN	Specify the FQDN or IP address of AuthMinder Server.
WebFortauthentication.port.1 WebFortauthentication.port.2	Optional, Required only if CA AuthMinder is used.	■ SAML ■ SiteMinder ■ VPN	Specify the port at which AuthMinder Server is available. Default value: **9742**
WebFortauthentication.transport.1	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the protocol for AuthMinder Server. **Note:** It is recommended that the communication between AFM and AuthMinder be over SSL. Refer to the CA AuthMinder Installation and Deployment Guide for more information on how to configure AuthMinder for SSL. Possible values are: ■ TCP ■ SSL Default value: **TCP**
WebFortauthentication.serverCACertPEMPath.1	Optional, *Required only if* WebFortauthentication.transport.1=SSL and WebFort Server is configured for two-way SSL.	■ SAML ■ SiteMinder ■ VPN	Specify the complete path of the *certification authority* (CA) certificate file for AuthMinder Server. The file must be in .PEM format.

Parameter	Required/ Optional	Used By	Description
WebFortauthentication.clientCertKey P12Path.1	Optional, *Required only if* WebFortauthentication.transport.1=SSL and WebFort Server is configured for two-way SSL.	■ SAML ■ SiteMinder ■ VPN	Specify the path of the p12 file that contains the key and certificate of the client communicating with AuthMinder Server. This establishes a two-way SSL between the AuthMinder client and server.
WebFortauthentication.clientCertKey Password.1	Optional, *Required only if* WebFortauthentication.transport.1=SSL and WebFort Server is configured for two-way SSL.	■ SAML ■ SiteMinder ■ VPN	Specify the client key pair password to open the p12 file specified in the WebFortauthentication.clientCertKeyP12Path.1 parameter.
WebFortpool.lifo	Optional	■ SAML ■ SiteMinder ■ VPN	Determines whether or not the pool returns idle objects in the last-in-first-out (LIFO) order. Possible values are: ■ **true**: Idle objects are returned in the LIFO order ■ **false**: Idle objects are not returned in the LIFO order Default: **false**
WebFortpool.numPreCreate	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the number of connections to be created during pool initialization. Default: **0**

Parameter	Required/ Optional	Used By	Description
WebFortpool.numConnectFailuresToTriggerFailover	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the number of consecutive connection failures required to fallback to another pool. Default: **1**
Least Used AuthMinder Server Authentication Parameters			
WebFortpool.maxactive	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the maximum number of connections that can exist between AFM and AuthMinder Server. The number of connections should not exceed this value. Default value: **32**
WebFortpool.maxIdle	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the maximum number of idle connections that can be established between SDK and AuthMinder Server. Default value: **16**
WebFortpool.maxWaitTimeMillis	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the maximum amount of time (in milliseconds) that a request waits to establish the connection. The default value of -1 indicates that the thread will wait indefinitely. Default value: **-1**
WebFortpool.minEvictableIdleTimeMillis	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the minimum amount of time a connection might be idle in the pool before it is evicted by the idle connection evictor, if any. The default value of -1 indicates that the idle connection would not be evicted. Default value: **-1**
WebFortpool.timeBetweenEvictionRunsMillis	Optional	■ SAML ■ SiteMinder ■ VPN	The amount of time (in milliseconds) to sleep before checking the pool to evict the idle connections. The default value of -1 indicates that there would not be any connection eviction. Default value: **-1**

Parameter	Required/ Optional	Used By	Description
WebFortauthentication.connectionTimeout.1	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the time (in milliseconds) before AuthMinder Server is considered unreachable. Default value: **10000** (10 seconds)
WebFortauthentication.readTimeout.1	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the maximum time (in milliseconds) allowed for a response from AuthMinder Server. Default value: **30000** (30 seconds) **Note:** A value of **0** results in the request waiting for a connection indefinitely.
Most Used AuthMinder Server Issuance Parameters			
WebFortissuance.host.1 WebFortissuance.host.2	Optional, Required only if CA AuthMinder is used.	■ SAML ■ SiteMinder ■ VPN	Specify the FQDN or IP address of the server hosting the AuthMinder Issuance service.
WebFortissuance.port.1 WebFortissuance.port.2	Optional, Required only if CA AuthMinder is used.	■ SAML ■ SiteMinder ■ VPN	Specify the port at which the server hosting the AuthMinder Issuance service is available. Default value: **9742**

Parameter	Required/ Optional	Used By	Description
WebFortissuance.transport.1	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the protocol for the AuthMinder Issuance service. **Note:** It is recommended that the communication between AFM and AuthMinder be over SSL. Refer to the CA AuthMinder Installation and Deployment Guide for more information on how to configure AuthMinder for SSL. Possible values are: ■ TCP ■ SSL Default value: **TCP**
WebFortissuance.serverCACertPEMPath.1	Optional, *Required only if* WebFortissuance.transport.1=SSL	■ SAML ■ SiteMinder ■ VPN	Specify the complete path of the CA certificate file for AuthMinder Server. The file *must* be in .PEM format.

Parameter	Required/ Optional	Used By	Description
WebFortissuance.clientCertKeyP12Path.1	Optional, *Required only if* WebFortissuance.transport.1=SSL and WebFort Server is configured for two-way SSL.	■ SAML ■ SiteMinder ■ VPN	Specify the path of the p12 file that contains the key and certificate of the client communicating with AuthMinder Server. This would establish two-way SSL between the AuthMinder client and server.
WebFortissuance.clientCertKeyPassword.1	Optional, *Required only if* WebFortissuance.transport.1=SSL and WebFort Server is configured for two-way SSL	■ SAML ■ SiteMinder ■ VPN	Specify the client key pair password for the p12 file specified in the WebFortissuance.clientCertKeyP12Path.1 parameter.
Least Used AuthMinder Server Issuance Parameters			
WebFortissaunce.connectionTimeout.1	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the time (in milliseconds) before AuthMinder Server is considered unreachable. Default value: **10000** (10 seconds)
WebFortissuance.readTimeout.1	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the maximum time (in milliseconds) allowed for a response from AuthMinder. Default value: **30000** (30 seconds)

The following table describes the User Data Service (UDS) parameters. These settings control how AFM communicates with UDS.

Parameter	Required/ Optional	Used By	Description
uds.connection.pool.count	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the maximum number of connections maintained by AFM with the UDS Web service at any given time. Default value: **20**
uds.ssl.keystore.path	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the absolute path to the two-way SSL keystore for UDS.
uds.ssl.keystore.password	Optional *Required only if* uds.ssl.keystore.path parameter is set.	■ SAML ■ SiteMinder ■ VPN	Specify the password for the UDS keystore.
uds.ssl.truststore.path	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the absolute path to the two-way SSL truststore for UDS.
uds.ssl.truststore.password	Optional *Required only if* uds.ssl.truststore.path parameter is set.	■ SAML ■ SiteMinder ■ VPN	Specify the password for the UDS truststore.
UDS Web Services Parameters			
uds.user.management.webservice.protocol	Required	■ SAML ■ SiteMinder ■ VPN	Specify the protocol for connecting to UDS.

Parameter	Required/ Optional	Used By	Description
uds.user.management.webservice.host	Required	■ SAML ■ SiteMinder ■ VPN	Specify the IP address or the FQDN of UDS.
uds.user.management.webservice.port	Required	■ SAML ■ SiteMinder ■ VPN	Specify the port at which UDS is available.
uds.user.management.webservice.urlpattern	Required	■ SAML ■ SiteMinder ■ VPN	Specify the URL pattern for UDS.

The following table describes the SSL VPN parameters. These settings control how AFM communicates with an SSL-enabled VPN.

Parameter	Required/ Optional	Used By	Description
ssl.vpn.username.form.name	Required	■ VPN	Specify the form parameter name in which the username parameter (collected by AFM) must be passed to the VPN gateway. Default value: **username**
ssl.vpn.password.form.name	Required	■ VPN	Specify the form parameter name in which the password parameter (collected by AFM) must be passed to the VPN gateway. Default value: **password**

Parameter	Required/ Optional	Used By	Description
ssl.vpn.mandatory .form.names	Optional	■ VPN	Specify the form parameter name(s) in which the mandatory (or required) request parameters collected from the SSL VPN must be posted back by AFM to the VPN gateway. **Note:** Multiple form parameters can be specified with a comma as the delimiter. For example, if you specify the value as realm,type, then AFM collects both realm and type from the VPN request. Default value: **realm**

Parameter	Required/ Optional	Used By	Description
ssl.vpn.posturl.form.name	Optional *Required, if* ssl.vpn.form.post.url is specified.	■ VPN	Specify the form parameter name in which the posturl parameter must be passed to the VPN gateway. **Note:** The posturl parameter refers to the URL to which AFM posts the authentication response. Default value: **posturl**
ssl.vpn.form.post.url	Optional *Required, if* ssl.vpn.form.posturl.form.name is specified.	■ VPN	Specify the URL to which the authentication response should be posted back.
ssl.vpn.errormessage.form.name	Optional	■ VPN	Specify the parameter name from which AFM determines an error occurred at the VPN-end after successful authentication by AFM. In this case, the request is sent back to AFM. Default value: **errormessage**

The following table describes the RiskMinder Server-related parameters:

Parameter	Required/ Optional	Used By	Description
Most Used RiskMinder Parameters			
RiskFortHOST.1 RiskFortHOST.2	Optional, *Required only if* RiskMinder is used in the integrated solution	SAML	Specify the IP address or the FQDN of RiskMinder Server.
RiskFortPORT.1 RiskFortPORT.2	Optional, *Required only if* RiskMinder is used in the integrated solution	SAML	Specify the port at which RiskMinder Server is available. Default value: **7680**
RiskFortTRANSPORT_TYPE	Optional	SAML	Specify the protocol to connect to RiskMinder Server. **Note:** It is recommended that the communication between State Manager and RiskMinder be over SSL. Refer to the *CA RiskMinder Installation and Deployment Guide* for more information on how to configure RiskMinder for SSL. Possible values are: ■ TCP ■ TLS Default value: **TCP**
RiskFortCA_CERT_FILE	Optional, *Required only if* RiskFortTRANSPORT_TYPE=TLS	SAML	Specify the complete path of the CA certificate file for RiskMinder Server. The file *must* be in.PEM format.

Parameter	Required/ Optional	Used By	Description
RiskFortAuthAdditionalInputs_*key*	Optional	SAML	Specify additional inputs to RiskMinder for risk evaluation. *key* should be replaced with the key name. Only alphanumeric characters can be passed as keys and values for the additional input. **Note:** For ISO 8859 Character Sets support, use the addRfAuthAdditionalInputs method of the AbstractStateData class.
Least Used RiskMinder Parameters			
RiskFortCONNECTION_TIMEOUT	Optional	SAML	Specify the time (in milliseconds) before RiskMinder Server is considered unreachable. Default value: **30000** (30 seconds)
RiskFortREAD_TIMEOUT	Optional	SAML	Specify the maximum time (in milliseconds) allowed for a response from RiskMinder Server. Default value: **30000** (30 seconds)
RiskFortCONNECTION_RETRIES	Optional	SAML	Specify the maximum number of retries allowed to connect to RiskMinder Server. Default value: **3**
RiskFortUSE_CONNECTION_POOLING	Optional	SAML	Specify whether the connection pooling with RiskMinder Server is enabled or disabled. Possible values are: ■ **1**: Enabled ■ **0**: Disabled Default value: **1**

Parameter	Required/ Optional	Used By	Description
RiskFortMAX_ACTIVE	Optional	SAML	Specify the number of maximum connections that can exist between State Manager and RiskMinder Server. The number of connections should not exceed this value. Default value: **32**
RiskFortTIME_BETWEEN_CONNECTION_EVICTION	Optional	SAML	Specify the time (in milliseconds) after which the connection eviction thread will be executed to check and delete any idle RiskMinder Server connection. Default value: **900000** (90 seconds)
RiskFortIDLE_TIME_OF_CONNECTION	Optional	SAML	Specify the time (in milliseconds) after which an idle RiskMinder Server connection will be closed. Default value: **1800000** (3 minutes) **Note:** Ensure that the value of RiskFortTIME_BETWEEN_CONNECTION_EVICTION + RiskFortIDLE_TIME_OF_CONNECTION is less than the firewall connection timeout value.
RiskFortWHEN_EXHAUSTED_ACTION	Optional	SAML	Specify the behavior when the maximum number of supported connections have exhausted. Default value: **BLOCK**

The following table describes the AFM parameters:

Parameter	Required/ Optional	Used By	Description
Most Used AFM Parameters			
User Browser Resources			
DeviceIDType	Optional	■ SAML ■ SiteMinder	Specify the type of cookie that must be stored on the end-user's system. RiskMinder uses Device ID to register and identify the device that is used by the user during a transaction. 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 are: ■ httpcookie ■ flashcookie Default value: **httpcookie**
User Credential Settings			
ArcotUserIDType	Optional	■ SiteMinder	Specify the user ID to use for the ArcotID PKI authentication and risk evaluation. Possible values are: ■ **LoginID** : Indicates that the user ID entered in the authentication page is used for risk evaluation and ArcotID PKI authentication. ■ **FullDN**: Indicates that disambiguated user ID is used for risk evaluation and ArcotID PKI authentication. Default value: **LoginID**
Lifecycle Settings			
MigrationMessage DisplayTimeLimit	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the time limit in milliseconds for displaying the migration success message to the user before it proceeds further. Default value: **6000**

Parameter	Required/ Optional	Used By	Description
EnrollSuccess DisplayTimeLimit	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the time limit in milliseconds for displaying the enrollment success message to the user before it proceeds further. Default value: **6000**
FailureMessage DisplayTimeLimit	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the time limit in milliseconds for displaying the failure message to the user (in case of any credential expiry, locked, or disabled credential) before redirecting back to the caller. Default value: **6000**
ProvisionAOTPPage URL	Required	■ SAML ■ SiteMinder ■ VPN	Specify the URL to issue ArcotID OTP through a mobile device. Default value: **/arcotafm/controller_aotp.jsp**
EnrollSuccessPage URL	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the path of the page that must be displayed after successful user enrollment. This parameter is valid only when **returnurl** parameter is not present in the request. It is useful when a user is going through the registration workflow and not the migration workflow. You must specify this parameter for SiteMinder direct enrollment. Default value: **/arcotafm/success.jsp**

Parameter	Required/ Optional	Used By	Description
Notification Settings			
sms.service.impl	Required	■ SAML ■ SiteMinder ■ VPN	Specify the implementation class for the SMS Service Provider. This class should implement the com.arcot.integrations.frontend.SMSService interface. **Important!** By default, this parameter is set to use the ClickATell SMS Service, which is provided for testing purposes only. It is recommended that you not use the default settings for production deployments.

Parameter	Required/ Optional	Used By	Description
email.service.impl	Required	■ SAML ■ SiteMinder ■ VPN	Specify the implementation class for the email Service Provider. This class should implement the com.arcot.integrations.frontend.EmailService interface. **Important!** By default, this parameter is set to use the ClickATell SMS Service, which is provided for testing purposes only. It is recommended that you not use the default settings for production deployments.
email.from.address	Required	■ SAML ■ SiteMinder ■ VPN	Specify the sender's email ID. Default value: **Do_Not_Reply@arcot.com**
email.from.name	Required	■ SAML ■ SiteMinder ■ VPN	Specify the sender's name. Default value: **Authentication Flow Manager**

Parameter	Required/ Optional	Used By	Description
email.smtp.host.name	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the FQDN or IP address of the server hosting the SMTP email service.
email.smtp.user.name	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the user name to access the SMTP email service.
email.smtp.user.password	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the password to access the SMTP email service.
email.smtp.isauth	Optional	■ SAML ■ SiteMinder ■ VPN	Specify whether or not user authentication is required to send email notification.

The following table describes the Utility parameters:

Parameter	Required/ Optional	Used By	Description
StopActionMode	Optional	■ SAML ■ SiteMinder ■ VPN	This option enables you to stop the automatic posting or redirecting of the AFM pages. The pages include a button that you must click to proceed to the next page. Possible values are: ■ true ■ false Default value: **false**

Parameter	Required/ Optional	Used By	Description
MaxStateMachine LoopCount	Optional	■ SAML ■ SiteMinder ■ VPN	Specify the maximum number of loops allowed in the state machine before an error is thrown to indicate an infinite loop condition. Default values: **100**

AFM Log File

To configure the log file for AFM, perform the following steps:

1. Navigate to the following directory on the system where you have installed AFM:

   AFM_HOME/conf/afm/

2. Open the arcotafm-log4j.properties file in a text editor, and set the log information, as described in the following table:

Parameter	Description
log4j.appender.afmout. File	Specify the log file name and the location where the AFM log files must be created. By default, on Apache Tomcat, the AFM log file name is arcotafm.log and it is created in the *AFM_HOME*/logs directory.

SAML Properties File

To manually configure the SAML properties, perform the following steps:

1. Navigate to the following directory on the system where you have installed AFM:

   AFM_HOME/conf/afm/

2. Open the saml_config.properties file in a text editor.

3. Make changes in the properties file by setting the parameters, as described in the following table:

Parameter	Required / Optional	Description
SamlIssuer	Required	Specify an identifier for the Issuer of SAML response that is making the claim(s) in the assertion. This property would set the SAML ISSUER tag. For example, ArcotCSSO.

Parameter	Required / Optional	Description
SamlStartLag	Optional	Specify the time (in milliseconds) to calculate the NotBefore time of an assertion. This is used in the condition when a valid assertion gets rejected because of skew of the time clocks between IdP and SP. Defaults value: **0**
SamlResponseValidity	Optional	Specify the time (in milliseconds) for which the SAML response issued by AFM is valid. Default value: **300000** (5 minutes)
SignSamlAssertionOnly	Optional	Specify whether the complete SAML response or only the assertion part of the response needs to be signed. If the complete response needs to be signed, set this property to false. Default value: **true** (only the SAML assertion would be signed)
CanonicalizationMethod	Optional	Specify the canonicalization method that is applied to the SAML response before signing it. Default value: **ALGO_ID_C14N_EXCL_WITH_COMMENTS**
SignatureMethod	Optional	Specify the signing algorithm used to sign the SAML response. Default value: **ALGO_ID_SIGNATURE_RSA_SHA1**
Audience	Optional	Specify the comma-separated (,) list of identifiers that can use the SAML response for taking any access decisions. If not specified, then only the issuer is added to the audience in the SAML response.

Parameter	Required / Optional	Description
AssertionConsumerServiceURL	Optional	Specify the URL where the SAML response (generated after authentication) has to be redirected. If the Service Provider is not sending this in the SAML request, then this property has to be configured. If the incoming SAML request has a value for the AssertionConsumerServiceURL, then that takes precedence over the configured value.
LogoutResponseRedirectURL	Optional	Specify the URL where the SAML logout response is sent after completing the logout procedure. This is not required if the logout request is processed through the Web service.
SamlIDPKeyStore	Required	Specify the absolute or relative path of the Identity Provider's key store file on the file system. This file has both the private key and certificate that are used to sign the SAML response. The syntax to specify the relative path is: /samlcerts/IDP.keystore
SamlIDPKeyStoreAlias	Required	Specify an alias of the private key and certificate stored in the Identity Provider's keystore. Default value: **arcotadapter**
SamlIDPKeyStorePassword	Required	Specify the password for the keystore of the Identity Provider. Default value: **123456**
SamlSPTrustStore	Optional, if SamlSPSignVerifyCert is configured	Specify the absolute or relative path of the trust store file of the Service Provider. This file has a certificate that is used to verify the signed SAML requests from the Service Provider. The syntax to specify the relative path is: /samlcerts/SP.truststore

Parameter	Required / Optional	Description
SamlSPTrustStoreAlias	Optional, *Required only if* SamlSPTrustStore is configured	Specify the alias with which the certificate is stored in the truststore of the Service Provider. Default value: **arcotadapter**
SamlSPTrustStorePassword	Optional, *Required only if* SamlSPTrustStore is configured	Specify the password for the truststore of the Service Provider. Default value: **123456**
SamlSPSignVerifyCert	Optional, if SamlSPTrustStore is configured	Specify the absolute or relative path of the X.509 certificate of the Service Provider. This is used to verify the signed SAML requests from the Service Provider. The syntax to specify the relative path is: /samlcerts/spcert.cer

Authentication Shim Properties File

The Authentication Shim configurations are performed in the adaptershim.ini file. This file defines the configuration parameters that must be set for Adapter and SiteMinder to communicate with each other. The file is available at the following location on the system where you have installed Authentication Shim:
installation_dir/conf

The section [arcot/integrations/smadapter/Default] contains the parameters that you need to set according to the authentication workflow that you want to use. The following table explains the parameters of this section:

Parameter	Required/ Optional	Description
PasswdSvcUserAtt	Optional	Specify a valid LDAP attribute of string type which has read-write access. This attribute *must not* be used by any other application. **Note:** This parameter is required only for authentication workflows using LDAP and when the password services are enabled in SiteMinder.
DisambigSchemeLib	Optional	Specify the DLL library name of an authentication scheme to use for user disambiguation. **Note:** This parameter does not support the refresh option. This means that 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 that 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 the refresh option. This means that if you switch to use Adapter authentication, then you must restart the SiteMinder Policy Server. ■ This parameter is not used for the delegated authentication scenario.

Parameter	Required/ Optional	Description
AuthSchemeParam	Optional	If you have configured a backing authentication scheme, this parameter is passed as the configuration string to the backing authentication scheme. This parameter must be set to have the same content that the SiteMinder Policy Server would set from the scheme configuration dialog. You can determine this by examining the scheme setup dialog boxes in the SiteMinder Policy Server administration interface. As you change parameters, the dialog box shows the parameter that the SiteMinder Policy Server would send. **Note:** This parameter is not used for the delegated authentication scenario.
ArcotSMBaseURL	Required	Specify the URL where State Manager is available. The syntax to specify State Manager URL is: https://*host_name:port_number*/arcotsm/servlet/
ArcotSMRetries	Optional	Specify the maximum number of retries allowed to connect to State Manager. If this value is 0, it signifies that only one connection attempt is allowed. Default value: **0**
ArcotSMResponseWait	Required	Specify the time period (in seconds) for which Authentication Shim will wait for State Manager to respond before logging an error. Default value: **5**
ArcotSMTrustedRootPEM	Required, *if* HTTPS is enabled	Specify the location of the certificate of the trusted root certificate authority, if State Manager is enabled for HTTPS. The file *must* be in .PEM format.
ArcotSMClientSSLCert	Required, *if* HTTPS is enabled	Specify the location of the client-side SSL certificate, if State Manager is enabled for HTTPS. The file *must* be in .PEM format.
ArcotSMClientPrivateKey	Required, *if* HTTPS is enabled	Specify the private key of the client in .PEM format, if State Manager is enabled for HTTPS. The file *must* be in .PEM format.

Parameter	Required/ Optional	Description
ArcotAFMLandingURL	Required	The controller JSP URL of AFM. **Note:** Although you can use multiple sample flows, you can configure only one ArcotAFMLandingURL per section.
UseCustomizationEngineAuth	Optional	Specify whether AFM is used to perform authentication. 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 is displayed to the user in case of an error.
InitialFCCURL	Required	Specify the URL of the initial FCC page served to the user. Authentication Shim reports this URL to SiteMinder during initialization. When the user attempts to access a protected resource and authentication is required, SiteMinder directs the user to this page. Depending on the authentication workflow, the page can collect information, such as the username or username and password.
FinalFCCURL	Required	Specify the URL that is used by AFM to forward the control back to Authentication Shim. 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 the [arcot/integrations/smadapter] section.

Parameter	Required/ Optional	Description
WatchInterval	Required	Specify the polling interval (in seconds) for Authentication Shim to use for monitoring the configuration file. Authentication Shim allows configuration changes without restarting SiteMinder Policy Server. It monitors the configuration file at this interval and if the file has changed, it reloads the configuration. Default value: **300**
ShimIdentifierString	Optional	Specify a unique identifier for the Authentication Shim instance. The value that you specify is appended with the section name to create an identifier.
LogSupported	Required	Specify whether to enable logging for Authentication Shim. Set this to **1** if you want to enable logging, or set this value to **0** to disable logging.
MultipleUserDirectoriesSupported	Optional	Specify whether to enable multiple user directory support. If this parameter is set to **1**, then multiple user directory support is enabled. Default value: **0** (disabled)
UserStatusFlag	Optional	Specify the user attribute in the directory server used by SiteMinder to store the user's status. **Note:** This parameter is required to enable detailed logging of user status in SiteMinder audit logs and Authentication Shim logs. The value of this parameter must match the value specified for the **Disabled Flag(RW)** attribute under the User Attributes tab in the SiteMinder User Directory Dialog.

Parameter	Required/ Optional	Description
SmApiVersion	Optional	Specify the supported version of the SiteMinder API. Supported versions are: ■ 300 ■ 400 ■ 401 Default value: **400** **Note:** If you change this value, restart the Policy Server for the changes to take effect.
SMPSLogEnabled	Optional	Specify whether to enable logging to the SiteMinder Policy Server log. Set the value to 1 if you want to enable logging to the SiteMinder Policy Server log. Set the value to 0 if you do not want to enable logging to the SiteMinder Policy Server log. Default value: 1 (enabled)
SMTraceLogEnabled	Optional	Specify whether to enable logging to the SiteMinder trace log. Set the value to 1 if you want to enable logging to the SiteMinder trace log. Set the value to 0 if you do not want to enable logging to the SiteMinder trace log. Default value: 1 (enabled)

Configuring the Log Information

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

Parameter	Required/ Optional	Description
DLLName	Optional	Specify 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 run time. Default value: **ArcotLog2FileSC**
HandleLevel	Optional	Specify the log level, which defines the details that must be included in the log messages. Messages with the specified severity level and higher levels are logged. For example, if the value is set to 2, then the messages of severity level 2 to 7 are logged. Supported values are: ■ 1=low ■ 2=info ■ 3=notice ■ 4=warning ■ 5=error ■ 6=alert ■ 7=fatal Default value: **3**
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 number of parameters to pass to the logging object. Default value: **4**

Parameter	Required/ Optional	Description
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 roll over the log file to a backup file. Supported values are: ■ HOURLY ■ DAILY ■ WEEKLY ■ MONTHLY **Note:** The LOG_FILE_ROLLOVER_INTERVAL parameter and the MAX_LOG_FILE_SIZE parameter (described in the next row) are both mutually exclusive. If you set one of these parameters, then you must comment the other one. The LOG_FILE_ROLLOVER_INTERVAL parameter is commented by default.

Parameter	Required/ Optional	Description
Param2=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 that 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. In addition, the MAX_LOG_FILE_SIZE parameter and the LOG_FILE_ROLLOVER_INTERVAL parameter (described in the previous row) are both mutually exclusive. If you set one of these parameters, then you must comment the other one. The MAX_LOG_FILE_SIZE parameter is enabled by default.
Param3=BACKUP_LOG_FILE_LOCATION	Optional	Specify the complete path where the backup log file is stored. The path provided must be valid. Default value: **installation_dir/logs/backup**

Parameter	Required/ Optional	Description
Param4=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 are: ■ LTZ=System Timezone, Date, and Time ■ SEV=Severity ■ PID=ProcessID ■ TID=ThreadID ■ MID=MessageIDNumber ■ MSG=Log Message Text ■ LID=LoggingID

Appendix C: Deploying and Configuring the Custom Application

Adapter is also shipped with a Custom Application, which can be used to verify the user enrollment and authentication workflows. The Custom Application is a standalone application and does not require you to integrate it with any other non-adapter components.

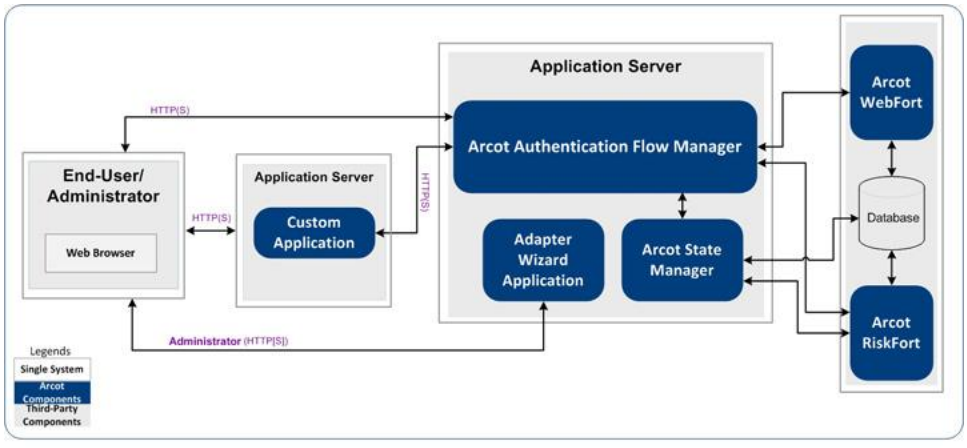
Important! Custom Application must not be used in production deployments. The Custom Application is provided to demonstrate the AFM workflows.

This appendix covers the following topics:

- Custom Application Deployment Architecture (see page 159)
- Deploying the Custom Application WAR Files (see page 160)
- Verifying the Custom Application Deployment (see page 161)
- Configuring the Custom Application (see page 162)

Custom Application Deployment Architecture

The following depicts *possible* deployment option for the Custom Application and the required Adapter components:



Install and deploy Custom Application and Adapter components as depicted in this figure.

Deploying the Custom Application WAR Files

To deploy Custom Application:

1. Navigate to the following location:

   sample_app_installation_dir/sampleApplications

2. Copy the customapp.war file to your application server. For example on Apache Tomcat, the location to copy the WAR file is:

   application_server_home/**webapps**

   Restart Apache Tomcat to extract the WAR file and to create a folder named customapp under the webapps folder.

   Note: Refer to the vendor documentation for instructions on how deploy on other supported application servers.

3. Copy the **customapp.properties** file from the place where you ran the AFM Wizard to the following location:

   AFM_HOME/conf/afm

4. (**Applicable Only for IBM WebSphere 6.1**) Perform the following steps to deploy WAR file on WebSphere 6.1:

   a. Log in to the IBM WebSphere administration console.

   b. Navigate to **Applications** > **Install New Application**.

   c. In the **How do you want to install the application** section, select the **Show me all installation options and parameters** option.

   d. Click **Next**.

   e. Click **Next** on the Preparing for the application installation screen.

   f. Click **Continue** on the Application Security Warnings screen.

   g. In the Step 1: Select install options screen, select the **Precompile JavaServer Pages files** option.

   h. Click **Next**.

   i. Click **Next** on the Step 2: Map modules to servers screen.

   j. In the Step 3: Provide options to compile JSPs screen, enter the value **15** in **JDK Source level** column.

   k. Follow the on-screen instructions and complete the deployment.

5. (**Applicable Only for IBM WebSphere 6.1**) Perform the following steps after you deploy the WAR file:

   a. Log in to the IBM WebSphere administration console.

   b. Navigate to **Applications** > **Enterprise Applications** > **WebSphere enterprise applications**.

c. Click the WAR file link.

d. Click the **Class loading and update detection** link.

e. In the **Class loader order** section, select the **Classes loaded with local class loader first** option.

f. In the WAR class loader policy section, select the **Single class loader for application** option.

g. Restart IBM WebSphere.

6. (**Applicable Only for IBM WebSphere 7.0**) Perform the following steps after you deploy the WAR file:

a. Log in to the IBM WebSphere administration console.

b. Navigate to **Applications** > **Application Types** > **WebSphere enterprise applications**.

c. Click the WAR file link.

d. Click the **Class loading and update detection** link.

e. In the **Class loader order** section, select the **Classes loaded with local class loader first (parent last)** option.

f. In the WAR class loader policy section, select the **Single class loader for application** option.

g. Restart IBM WebSphere.

Verifying the Custom Application Deployment

Access the following URL from the end-user's system:

http(s)://host_name:port_number/customapp/

Replace *host_name* and *port_number* with the host name and port of the system where you have deployed Custom Application. The main page of Custom Application opens.

If you see the welcome page of Custom Application, it indicates that you have successfully deployed Custom Application.

Configuring the Custom Application

After deploying Custom Application, you need to configure it before you can test it. To configure Custom Application, perform the following steps:

1. From the end-user's system, access Custom Application in a Web browser window. The default URL for Custom Application is:

   http[s]://host_name:port_number/customapp/

   The main page of Custom Application opens.

2. Click **Setup**.

   The Custom Application setup screen opens.

3. On the setup page, provide the following information:

   a. **Arcot AFM Protocol**: Select a protocol for establishing the communication channel with the application server hosting the AFM.

      Note: If you are using ArcotID PKI Flash client, then you must select the **https** protocol. For more information about ArcotID PKI Flash client, see the ArcotID Client Reference Guide available with the CA AuthMinder documentation.

   b. **Arcot AFM Host**: Specify the FQDN or IP address of the application server hosting the AFM.

   c. **Arcot AFM Port**: Specify the port at which the application server hosting the AFM is available.

   d. **Flow type**: Select an AFM profile from the list of available profiles that is displayed in the drop-down list. These profiles would have been created at the time of configuring Adapter. For information about creating AFM profiles, see Performing Adapter Configuration Using the Wizard (see page 47).

4. Click **Submit**.

   The "Setup Successful" message opens.

Testing the Custom Application

To test the Custom Application:

1. From the end-user's system, launch a new instance of the Web browser and access the main page of Custom Application by using the following URL:

   http[s]://host_name:port_number/customapp/

   Replace *host_name* and *port_number* with the host name and port of the system where you have deployed Custom Application.

   The main page of Custom Application opens.

2. Click the **Custom Application** link.

   Depending on the Flow Type you selected, you will be redirected to the AFM page for authentication. If you see the AFM page, it indicates that you have successfully configured the Custom Application.

Appendix D: Additional Configurations to Support LDAP Repository in AuthMinder

This appendix covers the following topics:

- Creating Organization in LDAP Repository (see page 166)
- Resolving Credential Types for LDAP Organization (see page 171)
- Verifying the LDAP Configuration in AuthMinder (see page 171)

Creating Organization in LDAP Repository

You must use Administration Console to support LDAP user directories. You must do this after you have successfully configured AuthMinder Server and Administration Console for AuthMinder.

1. Log in to Administration Console as *Master Administrator* by using the following URL:

   *http[s]://host_name:port_number/arcotadmin/***masteradminlogin.htm**

   In the preceding URL, *host_name* indicates the host name or the IP address of the application server where you configured the Administration Console and *port_number* indicates the port at which the server listens to incoming requests.

2. Create a Global Administrator account and assign only the **DEFAULTORG** to this administrator.

3. Log out of Administration Console.

4. Access AuthMinder Administration Console for the Global Administrator by using the following URL:

   *http[s]://host_name:port_number/arcotadmin/***adminlogin.htm**

5. Provide the organization name as DEFAULTORG and the username and password assigned to the global user account that you created in Step 2.

   You will be prompted to reset your password and login again to the Administration Console.

6. Click the **Organizations** tab.

7. Under the **Manage Organizations** section, click the **Create Organization** link to display the Create Organization page.

8. Enter the details of the organization, as described in the following table:

Field	**Description**
Organization Information	
Organization Name	Enter a unique ID for the organization that you want to create. Ensure that you specify this organization name in the Name (Mapped to LDAP) field described in the table in Configuring Adapter by Using the Wizard (see page 50). **Note:** You can use Administration Console to log in to this organization, by specifying this value, not the Display Name of the organization.
Display Name	Enter a descriptive name for the organization. **Note:** This name appears on all other Administration Console pages and reports.

Field	Description
Description	Provide a description for the administrators who will manage this organization. **Note:** You can provide additional details for later reference for the organization by using this field.
Administrator Authentication Mechanism	Select the **Basic User Password** mechanism to authenticate administrators belonging to this organization.
User Data Location	
Repository Type	Select **Enterprise LDAP**. By specifying this option, the user and administrator details for the new organization will be stored in the LDAP repository that you will specify on the next page.

9. Click **Next.**

   The Create Organization page to collect the LDAP repository details opens.

10. Enter the details, listed in the following table, to connect to the LDAP repository.

Field	Description
Host Name	Enter the host name of the system where the LDAP repository is available.
Port Number	Enter the port number on which the LDAP repository service is listening.
Schema Name	Specify the LDAP schema used by the LDAP repository. This schema specifies the types of objects that an LDAP repository can contain, and specifies the mandatory and optional attributes of each object type. Typically, the schema name for Active Directory is user and for SunOne Directory server it is inetorgperson.
Base Distinguished Name	Enter the base Distinguished Name of the LDAP repository. This value indicates the starting node in the LDAP hierarchy to search in the LDAP repository. For example, for SunOne Directory server to search or retrieve a user with a DN of cn=rob laurie, dc=Test,dc=Pvt, you must specify the Base Distinguished Name as: dc=Test,dc=Pvt **Note:** Typically, this field is case sensitive and searches all sub-nodes under the provided base DN.

Field	Description
Redirect Schema Name	Specify the name of the schema that provides the definition of the "member" attribute. You can search for users in the LDAP repository using the Base DN defined for an organization. But this search only returns users belonging to the specific Organization Unit (OU). An LDAP administrator might want to create a group of users belonging to different Organization Units for controlling access to an entire group, and might want to search for users from different groups. When the administrator creates groups, user node DNs are stored in a "member" attribute within the group node. By default, UDS does not allow search and DN resolution based on attribute values. Redirection enables you to search for users belonging to different groups within LDAP, based on specific attribute values for a particular node. Typically, the redirect schema name for Active Directory is group and for SunOne directory it is groupofuniquenames.
Connection Type	Select the type of connection that you want to use between Administration Console and the LDAP repository. Supported types are: ■ TCP ■ One-way SSL ■ Two-way SSL
Login Name	Enter the complete distinguished name of the LDAP repository user who has the privilege to log into the repository server and manage the Base Distinguished Name. The following example shows how to specify the Login Name for SunOne Directory server: cn=Directory Manager
Login Password	Enter the password of the user provided in the Login Name.
Server Trusted Root Certificate	Enter the path for the trusted root certificate who issued the SSL certificate to the **LDAP** server by using the **Browse** button, if the required SSL option is selected.
Client Key Store Path	Enter the path for the key store that contains the client certificate and the corresponding key by using the Browse button, if the required SSL option is selected. **Note:** You must upload either PKCS#12 or JKS key store type.
Client Key Store Password	Enter the password for the client key store, if the required SSL option is selected.

1. Click **Next** to proceed.

   The page to map the repository attributes opens.

2. On this page:

   a. Select an attribute from the **Arcot Database Attributes** list, then select the appropriate attribute from the **Enterprise LDAP Attributes** list that needs to be mapped with the Arcot attribute, and click **Map**.

      Important! Mapping of the USERNAME, EMAILADDR, and TELEPHONENUMBER attributes is compulsory. If you are using SunOne Directory, then map USERNAME to uid, EMAILADDR to mail, and TELEPHONENUMBER to telephoneNumber.

   b. Repeat the process to map multiple attributes, until you finish mapping all the required attributes.

      Note: You do not need to map all the attributes in the **Arcot Database Attributes** list. You only need to map the attributes that you will use.

      The attributes that you have mapped will be moved to the **Mapped Attributes** list.

      If required, you can unmap the attributes. If you want to unmap a single attribute at a time, then select the attribute and click **Unmap**. However, if you want to clear the **Mapped Attribute** list, then click **Reset** to unmap all the mapped attributes.

3. Click **Next** to proceed.

   The Select Attribute(s) for Encryption screen opens.

4. Select the attributes that you want to encrypt, and click **Next**.

   The Add Administrators screen opens.

   Note: This page is *not* displayed, if all the administrators currently present in the system have scope to manage all organizations.

5. From the **Available Administrators** list, select the administrators who will manage the organization and click the **>** button to add the administrator to the **Managing Administrators** list.

   Note: Assigning organization to administrators can be done at any time by updating the scope of existing administrators or by creating new administrators to manage the organization.

   The **Available Administrators** list displays all the administrators who can manage the new organization.

   Note: If some administrators have scope to manage all organizations in the system, then you will not see the corresponding entries for those administrators in this list.

   The **Managing Administrators** list displays the administrators that you have selected to manage this organization.

6. Click **Next** to proceed.

The Activate Organization screen opens.

Note: The username attribute *cannot* be changed or updated after the organization is activated.

7. Click **Enable** to activate the new organization.

   The message box opens.

8. Click **OK** to complete the process.

9. Refresh the AuthMinder cache for changes to take effect.

   Now if you perform a search for organizations, in the search result, you will see the LDAP-based organization you created.

10. Create a user in this organization.

11. Search for the user created in the preceding step and promote that user to Global Administrator (GA).

    Note: Refer to the Promoting Users to Administrators section in the CA AuthMinder Administration Guide for more information.

    You will need the details of this GA to resolve the credential types for the LDAP-based organization. See Resolving Credential Types for LDAP Organization (see page 171) for more information.

12. Log out of the Administration Console.

Resolving Credential Types for LDAP Organization

The authentication requests that are presented to the AuthMinder Server must specify the type of credential that has to be used to process the request. If the input requests are presented with the unknown credential type, then such requests are resolved to any password-based mechanism supported by AuthMinder.

To resolve the credential types for the LDAP-based organization created in Creating Organization in LDAP Repository (see page 166):

1. Ensure that you are logged in as the Global Administrator (GA) created in Creating Organization in LDAP Repository (see page 166).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Miscellaneous Configurations section, click the Credential Type Resolution link to display the Credential Type Resolution Configuration page.
5. In this page:
   - Create a new configuration with the name, for example, LDAPResolution.
   - In the Resolve Plain to field, select LDAP Password.
6. Save the configuration.
7. Apply this configuration using the Assign Default Configurations page.

Note: Refer to the Assigning Default Configurations section in the CA AuthMinder Administration Guide for more information.

Verifying the LDAP Configuration in AuthMinder

To verify the LDAP organization and user configuration:

1. Log in to AuthMinder Sample Application by using the following URL:

   http[s]://host:port/webfort-7.1.01-sample-application/
2. In the left pane, click Password > Authentication > Complete Password to open the Password Authentication page.
3. Enter the LDAP user name, organization, and password.
4. Click Authenticate.

   The Authentication Response Details screen opens.

   If you see the details of the LDAP user, it indicates that you have successfully configured LDAP support in AuthMinder.

Appendix E: Configuring SSL in Apache Tomcat

For security purposes, it is recommended that you enable SSL between different Adapter components. To do this, you must enable the application server where Adapter components are deployed for SSL communication.

For testing purposes, you can use the default certificates shipped with the Adapter package to enable the SSL communication between the Adapter components. These certificates are available in the **certs** folder of the installation directory.

This appendix walks you through the following topics:

- Configuring SSL
- Verifying the SSL Configuration in Tomcat

Configuring SSL

Authentication Flow Manager (AFM) and State Manager components are installed on the application server. Therefore, to enable SSL for these components, you have to configure the application server where these components are deployed for SSL.

To enable Authentication Shim to communicate over SSL, you must set the following configuration parameters in the **adaptershim.ini** file:

- ArcotSMTrustedRootPEM
- ArcotSMClientSSLCert
- ArcotSMClientPrivateKey

To enable Apache Tomcat for SSL

Important! If you are integrating Adapter with the SAML-based Web portal, then you must also perform this task on the Service Provider's system.

1. Browse to the following location on the system where you have installed State Manager:

   state_manager_installation_dir/adapterStateManager/**certs**

2. Copy the **server.keystore** file on the system where AFM is installed. For example, copy this file into a temporary folder called /**arcottemp**/**certificate**.

3. Navigate to the following location on the system where AFM is installed:

   Tomcat_root/**conf**

   Note: *Tomcat_root* refers to the Apache Tomcat installation directory. Refer to the vendor documentation for instructions on how deploy on other supported application servers.

4. Open **server.xml** file in a text editor.

5. Search for the following code:

```
<!--
        <Connector port="8443" protocol="HTTP/1.1"
   SSLEnabled="true"
                maxThreads="150" scheme="https" secure="true"
                clientAuth="false" sslProtocol="TLS" />
-->
```

   Replace the code with

```
<Connector SSLEnabled="true" clientAuth="false"
keystoreFile="/arcottemp/certificate/server.keystore"
keystorePass="123456" maxThreads="150" port="8443"
protocol="HTTP/1.1" scheme="https" secure="true"
sslProtocol="TLS"/>
```

6. (Only for Apache Tomcat 7.x) If you are configuring SSL on Apache Tomcat 7.x, you might see an error with default configurations. In this case, you must:

a. Delete the bin/tcnative-1.so file.

b. In server.xml, search for and remove the following line:

```
<Listener
className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

7. Save and close server.xml.
8. Restart Apache Tomcat.

Verifying the SSL Configuration in Tomcat

From the end-user's system, access the following URL:

https://host_name:port_number/

Replace *host_name* and *port_number* with the host name and the SSL port that you configured on the system where you have installed Apache Tomcat (on the system hosting AFM and if configured on Service Provider's system). You should see the Apache Tomcat home page.

Note: Because the certificates shipped with Adapter package are for testing purposes only, you will notice the Certificate Error on accessing this page. You can safely ignore this error.