This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
CA Technologies Product References

This document references the following CA Technologies products:

- CA Arcot™
- CA Arcot RiskFort™
- CA Arcot WebFort®
- CA SiteMinder®

Contact CA Technologies

Contact CA Support

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

- 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

Provide Feedback

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

If you would like 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: CA Arcot WebFort and RiskFort

- Authentication in an On-Premise Arcot Integration .................................................. 8
- Confidence Levels and SiteMinder Authorization ..................................................... 9
- Risk Scores and Confidence Levels Compared ......................................................... 10
- CA Arcot Integration Use Cases .................................................................................. 11
  - CA Arcot Authentication and Risk Analysis ......................................................... 11
  - SiteMinder Authentication and CA Arcot Risk Analysis ....................................... 13
  - SiteMinder Authorization and Confidence Levels .................................................. 14
- User Store Consideration ............................................................................................ 15
- Add a Confidence Level to a Policy ............................................................................. 15

## Chapter 2: CA Arcot A-OK

- Authentication in a Hosted CA Arcot Integration ..................................................... 18
- Confidence Levels and SiteMinder Authorization ..................................................... 18
- Risk Scores and Confidence Levels Compared ......................................................... 19
- CA Arcot A-OK Integration Use Cases ....................................................................... 20
  - CA Arcot A-OK Authentication and Risk Analysis ............................................... 20
  - SiteMinder Authorization and Confidence Levels .................................................. 22
- User Store Consideration ............................................................................................ 22
- Add a Confidence Level to a Policy ............................................................................. 22
You use the CA Arcot Adapter™ (Adapter) to integrate SiteMinder with an on-premise implementation of the CA Arcot WebFort strong authentication solution and the CA Arcot RiskFort adaptive authentication solution.

Consider the following before you begin:

- The integration requires a minimum version of the Adapter and CA Arcot RiskFort.
- The integration requires a minimum version of CA Arcot WebFort.

**Note:** For more information about the supported versions, see the r12.0 SP3 SiteMinder Platform Support Matrix.

The purpose of the following diagram is to:

- Illustrate how the Adapter and its components, CA Arcot RiskFort, and CA Arcot WebFort integrate in a SiteMinder environment.
- Detail the major components and their general relationships.
Authentication in an On-Premise Arcot Integration

CA Arcot assumes authentication services in an integrated environment by guiding users through the authentication (CA Arcot WebFort) and risk evaluation (CA Arcot RiskFort) processes. During the authentication process:

- CA Arcot WebFort provides the strong authentication, which helps to ensure that the identities of the users requesting the SiteMinder–protected resources are legitimate.

Note: For more information about strong authentication, see the CA Arcot WebFort Installation and Deployment Guide. For more information about configuring the supported authentication methods, see the CA Arcot WebFort Administration Guide.

Figure 1: CA SiteMinder and CA Arcot integration architecture
CA Arcot RiskFort collects a range of data to complete a risk evaluation, which determines the level of risk associated with each transaction.

**Note:** For more information about risk evaluation and risk scores, see the *CA Arcot RiskFort Installation and Deployment Guide*. For more information about configuring risk scoring, see the *CA Arcot RiskFort Administration Guide*.

The result of the risk evaluation is a risk score and corresponding advice, which is a recommend action, such as allow or deny the authentication.

CA Arcot forwards the advice to the Policy Server, which if necessary, continues with its authorization services.

**Note:** For more information about the Adapter workflow and the role of each CA Arcot component during authentication, see the *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*.

---

**Confidence Levels and SiteMinder Authorization**

The Policy Server maintains authorization services in an integrated environment and can apply the risk score to authorization decisions. The risk score is created during the authentication process (see page 8).

The Policy Server applies the risk score as a SiteMinder confidence level (confidence level). A confidence level is based on a risk score, and as such, is also an integer that represents the likelihood that the transaction is safe.

The following example workflow details the relationship between both values and explains how the Policy Server applies a confidence level to authorization decisions:

1. After the user is successfully authenticated, the Adapter converts the risk score to a confidence level using the following algebraic formula:
   \[(100 - \text{risk score}) \times 10 = \text{confidence level}\]

2. The Adapter inserts the confidence level into the SiteMinder session ticket.
   **Note:** For more information about session tickets, see the *Policy Server Configuration Guide*.

3. As the user requests protected resources, the Policy Server compares the confidence level in the session to ticket to the confidence level configured in the policy.

4. The following can occur:
   - If the policy rule is configured to allow access and the user’s confidence level is equal to or greater than the confidence level configured in the policy, the policy rule is triggered.
**Risk Scores and Confidence Levels Compared**

Although a risk score and a confidence level both help to ensure that the transaction is safe, there are differences between both values. Consider the following differences when planning for authorization decisions:

<table>
<thead>
<tr>
<th>CA Arcot Risk Score</th>
<th>SiteMinder Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>A risk score is represented by a numeric scale 0–100.</td>
<td>A confidence level is represented by a numeric scale 0–1000.</td>
</tr>
<tr>
<td>The lower the risk score, the greater the chance that the transaction is safe.</td>
<td>The higher the confidence level, the greater the chance that the transaction is safe.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A value of zero (0) represents no confidence and results in SiteMinder denying access to the requested resource.</td>
</tr>
</tbody>
</table>

The following example workflow details the inverse relationship between a risk score and a confidence level:

1. A user requests a SiteMinder protected resource and is forwarded to CA Arcot for authentication.
2. The Adapter guides the user through authentication and risk analysis. Based on the CA Arcot evaluation and scoring rules, the user is authenticated with a risk score of 30. The lower risk score is representative of a safe transaction.

**Note:** For more information about risk evaluation and scoring rules, see the *CA Arcot RiskFort Administration Guide*. 
3. The Adapter:
   a. Forwards the authentication decision to the Policy Server
   b. Converts the risk score to a confidence level using the following algebraic formula:
      \[(100 - \text{risk score}) \times 10 = \text{confidence level}\]
      In this example, the Adapter converts the risk score to a confidence level using the following:
      \[(100 - 30) \times 10 = 700\]
      The higher confidence level is representative of a safe transaction.

4. The Adapter inserts the confidence level into the user session ticket.

5. The user requests a resource protected by a policy that requires a confidence level of at least 700.

6. The Policy Server grants access to the resource.

---

**CA Arcot Integration Use Cases**

The following use cases detail how you can integrate SiteMinder with CA Arcot strong authentication and risk evaluation. The use cases begin with a simple integration and progress into more complex scenarios.

---

**CA Arcot Authentication and Risk Analysis**

The simplest deployment includes integrating the Adapter and all related components with SiteMinder.

The Adapter guides users through the authentication (CA Arcot WebFort) and risk evaluation (CA Arcot RiskFort) processes to apply a risk score during authentication (see page 8).

**To deploy Arcot authentication and risk analysis**

1. Be sure that CA Arcot RiskFort and CA Arcot WebFort are installed and configured.
   
   **Note:** For more information, see the respective CA Arcot installation and deployment guide.

2. Install and deploy the CA Arcot Adapter and all related components. These components include a set of Forms Credential Collector files. These files let you use the Adapter HTML forms authentication scheme to gather user credentials.

   **Note:** For more information about installing and configuring the Adapter and all related components, see the *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*. 

---
3. Do the following:
   a. Configure a SiteMinder Custom authentication scheme to call the Adapter library.
   b. Determine which Web Agents are included in the CA Arcot integration and configure the respective Agent Configuration Objects (ACO) to support the integration.

   **Note:** For more information about the required custom authentication scheme and ACO settings, see the *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*. For more information about configuring an authentication scheme and ACO parameters, see the *Policy Server Configuration Guide*.

The following diagram illustrates this deployment scenario:

*Figure 2: CA Arcot authentication and risk analysis*
SiteMinder Authentication and CA Arcot Risk Analysis

You can configure the Adapter for risk evaluation only by integrating a SiteMinder authentication scheme. A SiteMinder authentication scheme that is part of the integration is known as backing authentication.

If you use a SiteMinder authentication scheme as backing authentication, the Shim acts as an interface between SiteMinder and the SiteMinder authentication scheme.

Note: For more information about backing authentication, see the CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide. Not all SiteMinder authentication schemes are supported for backing authentication. For more information, see the r12.0 SP3 SiteMinder Platform Support Matrix.

To deploy SiteMinder authentication and Arcot risk analysis

1. Complete the steps listed in CA Arcot Authentication and Risk Analysis (see page 11).
   Important! The integration requires that a SiteMinder Custom authentication scheme is configured. The SiteMinder Custom authentication scheme calls the required Adapter library. This library is required even if you are deploying backing authentication.

2. Be sure that you configure the SiteMinder Custom authentication scheme with a valid CA Arcot parameter. This parameter must represent a user flow that supports the SiteMinder authentication scheme that is functioning as backing authentication. You enter this value in in the Parameter field.
   Note: For more information about user flows and the corresponding parameter values, see the CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide. For more information about configuring a SiteMinder Custom authentication scheme, see the Policy Server Configuration Guide.

3. Configure the Shim to use the SiteMinder authentication scheme as a backing authentication.
   Note: For more information about configuring a backing authentication scheme, see the CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide.
SiteMinder Authorization and Confidence Levels

You can extend the Policy Server authorization services by adding a confidence level (see page 9) to policies. You add a confidence level to policies in the context of an active policy expression.

Adding a confidence level to policies lets you apply the CA Arcot risk analysis results to authorization decisions.

To add a confidence level to policies

1. Complete the steps in CA Arcot Authentication and Risk Analysis (see page 11) or SiteMinder Authentication and CA Arcot Risk Analysis (see page 13).

2. Create or modify a policy to include an active policy expression that references the following.
   - The CA Arcot risk analysis library (smriskactiveexpr).
   - A confidence level value of 1–1000.
More information:

Add a Confidence Level to a Policy (see page 15)

User Store Consideration

All SiteMinder users to which the integration applies must be made available to the CA Arcot WebFort database.

Contact CA Arcot Support for assistance.

Note: For contact information, see the CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide.

Add a Confidence Level to a Policy

You add a confidence level to a policy to apply the results of a risk evaluation to an authorization decision.

To add a confidence level to a policy
1. Open the policy.
2. Do the following in the Active Policy Expression area:
   a. Enter the following library name:
      smriskactiveexpr
   b. Enter the following function name:
      CheckConfidenceLevel
   c. Enter a confidence level in the Function Parameter(s) field. A valid value is 1-1000.
3. Click Submit.
Chapter 2: CA Arcot A-OK

You use the CA Arcot A–OK Adapter™ (A–OK Adapter) to integrate SiteMinder with the hosted CA Arcot A–OK service.

**Note:** The integration requires a minimum version of the A–OK Adapter. For more information about the supported version, see the r12.0 SP3 SiteMinder Platform Support Matrix.

The purpose of the following diagram is to:
- Illustrate how the A–OK Adapter and its components integrate in a SiteMinder environment.
- Detail the major components and their general relationships.

**Note:** For more information about installing and configuring the A–OK Adapter, see the CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide.

*Figure 4: CA SiteMinder and CA Arcot A-OK integration architecture*
Authentication in a Hosted CA Arcot Integration

CA Arcot A–OK assumes authentication services in an integrated environment by guiding users through the authentication and risk evaluation processes. CA Arcot A–OK uses a series of SAML requests and responses to step through the authentication workflow.

**Note:** For more information about the authentication workflow, see the *CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide*.

The result of the risk evaluation is a risk score and corresponding advice, which is a recommend action, such as allow or deny the authentication.

CA Arcot A–OK forwards the advice to the Policy Server, which if necessary, continues with authorization services.

**Note:** For more information about managing user credentials and configuring the rules associated with the risk evaluation process, see the *CA Arcot A–OK User Administration Guide*.

Confidence Levels and SiteMinder Authorization

The Policy Server maintains authorization services in an integrated environment and can apply the risk score to authorization decisions. The risk score is created during the **authentication process** (see page 18).

The Policy Server applies the risk score as a SiteMinder confidence level. A confidence level is based on a risk score, and as such, is also an integer that represents the likelihood that the transaction is safe.

The following example workflow details the relationship between both values and explains how the Policy Server applies a confidence level to authorization decisions:

1. After the user is successfully authenticated, the A–OK Adapter converts the risk score to a confidence level using the following algebraic formula:
   
   \[(100 - \text{risk score}) \times 10 = \text{confidence level}\]

2. The A–OK Adapter inserts the confidence level into the SiteMinder session ticket.

   **Note:** For more information about session tickets, see the *Policy Server Configuration Guide*.

3. As the user requests protected resources, the Policy Server compares the confidence level in the session to ticket to the confidence level configured in the policy.
4. The following can occur:
   - If the policy rule is configured to allow access and the user’s confidence level is equal to or greater than the confidence level configured in the policy, the policy rule is triggered.
     
     **Note:** If the user’s confidence level is less than the confidence level configured in the policy, SiteMinder denies access.
   
   - If the policy rule is configured to reject access and the confidence level is less than the value configured in the policy, the policy rule is triggered.

## Risk Scores and Confidence Levels Compared

Although a risk score and a confidence level both help to ensure that the transaction is safe, there are differences between both values. Consider the following differences when planning for authorization decisions:

<table>
<thead>
<tr>
<th>CA Arcot Risk Score</th>
<th>SiteMinder Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>A risk score is represented by a numeric scale 0–100.</td>
<td>A confidence level is represented by a numeric scale 0–1000.</td>
</tr>
<tr>
<td>The lower the risk score, the greater the chance that the transaction is safe.</td>
<td>The higher the confidence level, the greater the chance that the transaction is safe.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A value of zero (0) represents no confidence and results in SiteMinder denying access to the requested resource.</td>
</tr>
</tbody>
</table>

The following example workflow details the inverse relationship between a risk score and a confidence level:

1. A user requests a SiteMinder protected resource and is forwarded to CA Arcot A–OK for authentication.

2. The A–OK Adapter guides the user through authentication and risk analysis. Based on the CA Arcot A–OK evaluation and scoring rules, the user is authenticated with a risk score of 30. The lower risk score is representative of a safe transaction.

   **Note:** For more information about managing user credentials and configuring the rules associated with the risk evaluation process, see the *CA Arcot A–OK User Administration Guide*. 

3. The A–OK Adapter:
   a. Forwards the authentication decision to the Policy Server
   b. Converts the risk score to a confidence level using the following algebraic formula:
      \[(100 - \text{risk score}) \times 10 = \text{confidence level}\]
      In this example, the A–OK Adapter converts the risk score to a confidence level using the following:
      \[(100 - 30) \times 10 = 700\]
      The higher confidence level is representative of a safe transaction.

4. The A–OK Adapter inserts the confidence level into the user session ticket.

5. The user requests a resource protected by a policy that requires a confidence level of at least 700.

6. The Policy Server grants access to the resource.

CA Arcot A–OK Integration Use Cases

The following use cases detail how you can integrate SiteMinder with CA Arcot A–OK strong authentication and risk evaluation. The use cases begin with a simple integration and progress into more complex scenarios.

CA Arcot A–OK Authentication and Risk Analysis

The simplest deployment includes integrating the A–OK Adapter and all related components with SiteMinder.

The A–OK Adapter guides users through the authentication and risk evaluation processes to apply a risk score during the authentication process (see page 18). 

To deploy CA Arcot A–OK authentication and risk analysis

1. Be sure that the CA Arcot A–OK service is available.

2. Install and deploy the A–OK Adapter and all related components. These components include a set of Forms Credential Collector files. These files let you use the A–OK Adapter HTML forms authentication scheme to gather user credentials.

   **Note:** For more information about installing and configuring the A–OK Adapter and all related components, see the CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide.
3. Do the following:
   a. Configure a SiteMinder Custom authentication scheme to call the A–OK Adapter library.
   b. Determine which Web Agents are included in the CA Arcot A–OK integration and configure the respective Agent Configuration Objects (ACO) to support the integration.
   c. Add the A–OK Adapter JAR files, certificates, and properties files to the Policy Server’s Java Virtual Machine (JVM) file (JVMOptions.txt).

   **Note:** For more information about the required custom authentication scheme, ACO settings, and edits to the Policy Server JVM file, see the *CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide*. For more information about configuring an authentication scheme and ACO parameters, see the *Policy Server Configuration Guide*.

The following diagram illustrates this deployment scenario:

*Figure 5: CA Arcot A–OK authentication and risk analysis*
SiteMinder Authorization and Confidence Levels

You can extend the Policy Server authorization services by adding a confidence level (see page 18) to policies. You add a confidence level to policies in the context of an active policy expression.

Adding a confidence level to policies lets you apply the CA Arcot A–OK risk analysis results to authorization decisions.

To add a confidence level to policies
1. Complete the steps in CA Arcot A–OK Authentication and Risk Analysis (see page 20).
2. Create or modify a policy to include an active policy expression that references the following.
   ■ The CA Arcot A–OK risk analysis library (smriskactiveexpr).
   ■ A confidence level value of 1–1000.

More information:
Add a Confidence Level to a Policy (see page 15)

User Store Consideration

All SiteMinder users to which the integration applies must be made available to the CA Arcot A–OK hosted service.

Contact CA Arcot Support for assistance.

Note: For contact information, see the CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide.

Add a Confidence Level to a Policy

You add a confidence level to a policy to apply the results of a risk evaluation to an authorization decision.

To add a confidence level to a policy
1. Open the policy.
2. Do the following in the Active Policy Expression area:
   a. Enter the following library name:
      smriskactiveexpr
b. Enter the following function name:
   CheckConfidenceLevel

c. Enter a confidence level in the Function Parameter(s) field. A valid value is 1-1000.

3. Click Submit.