Computer Associates
CA SiteMinder 12.5

RSA SecurID Ready Implementation Guide

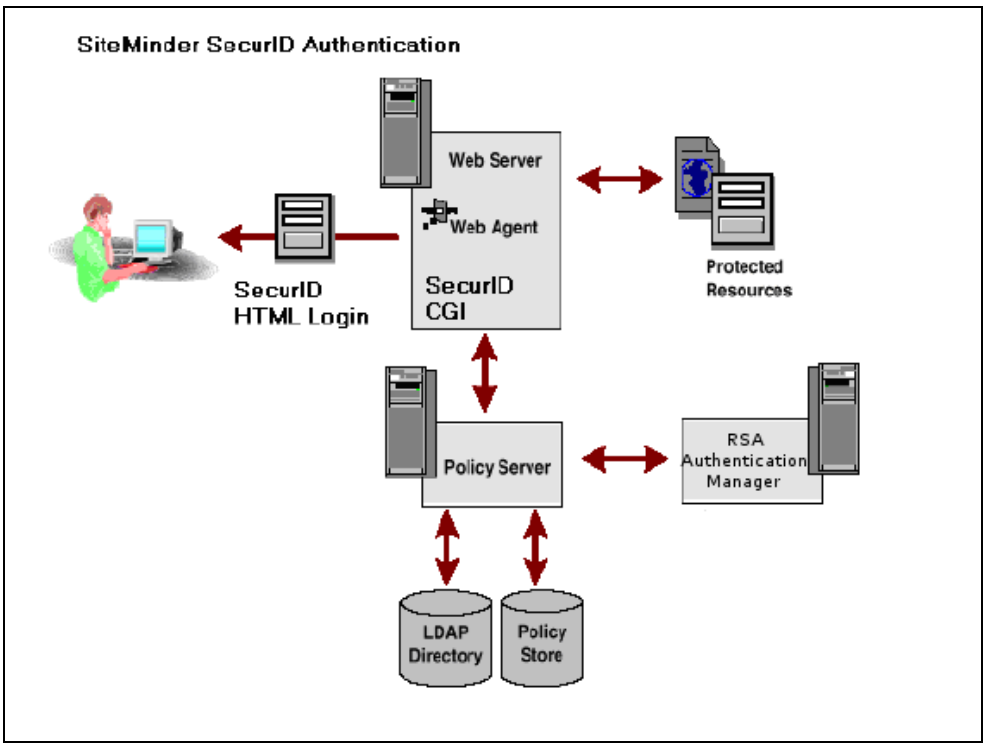
Last Modified: March 20, 2013

Partner Information

Product Information	
Partner Name	Computer Associates
Web Site	www.ca.com
Product Name	CA® SiteMinder®
Version & Platform	12.5
Product Description	CA® SiteMinder® provides a centralized security management foundation that enables user authentication and controlled access to Web applications and portals. CA SiteMinder delivers the market's most advanced security management capabilities and enterprise-class site administration, allowing you to reduce IT operational costs and enabling greater IT control and security. CA SiteMinder enables the secure delivery of essential information and applications to your employees, partners, suppliers and customers — and scales with your growing business needs.

Solution Summary

CA SiteMinder provides enterprises with the option to use RSA SecurID two-factor authentication when their users attempt to access SiteMinder-protected resources. To enable RSA SecurID authentication, a SiteMinder administrator can create an RSA SecurID scheme and associate it with protected resources contained within SiteMinder Realms. When a SiteMinder Web Agent detects that a user is attempting to access a resource located in one of these realms, it notifies the SiteMinder Policy Server. The Policy Server then prompts the user for a username and RSA SecurID passcode and passes the credentials to the RSA Authentication Manager Server for authentication.



Supported RSA Features CA SiteMinder 12.5	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	Yes
Risk-Based Authentication with Single Sign-On	Yes
RSA Authentication Manager Replica Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes

Authentication Agent Configuration

Authentication Agents are records that are stored in an RSA Authentication Manager server's database; they contain information that allows the server to locate its clients and establish secure communication channels with them. Use the RSA Security Console to create an agent record for each CA SiteMinder Web Agent in your environment.

You will need the following information in order to do so:

- the hostname of each SiteMinder Web Agent in your environment
- IP address for all of the network interfaces on each SiteMinder Web Agent host

Set each of your Authentication Agent's **Agent Type** to *Standard Agent*.

Note: Each agent hostname must resolve to one or more valid IP addresses on the local network.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	Windows*: %SYSTEM_32_ROOT%* Unix*: /var/ace*
Node Secret (*securid*)	Windows*: %SYSTEM_32_ROOT%* Unix*: /var/ace*
sdstatus.12	Windows*: %SYSTEM_32_ROOT%* Unix*: /var/ace*
sdopts.rec	Not implemented

Partner Product Configuration

Before You Begin

This section provides instructions for enabling RSA SecurID two-factor authentication for CA SiteMinder users. You should have working knowledge of CA SiteMinder Policy Server and RSA Authentication Manager, as well as access to the appropriate end-user and administrative documentation. Ensure that that both products are running properly prior to configuring the integration. Note that this document is not intended to suggest optimum installations or configurations.

Prerequisites

The instructions in this guide assume that you have installed/configured the following CA and RSA components in addition to CA SiteMinder Policy Server and RSA Authentication Manager.

CA SiteMinder Web Agent Prerequisites

You must install at least one CA SiteMinder Web Server Agent in your environment and register it with the CA Policy Server before proceeding. Consult the *CA SiteMinder Web Agents* guide for more information.

CA SiteMinder Policy Server Object Prerequisites

You must configure the following Policy Server system and domain policy objects before proceeding:

- one or more Agent Configuration Objects
- one or more Domains
- a User Directory

Note: You must map each of your RSA Authentication Manager user IDs to its corresponding CA SiteMinder user ID. The simplest way to accomplish this is to assign each user matching usernames. Consult the *CA Policy Server Configuration Guide* for more information.

RSA Authentication Agent Prerequisites

Follow the steps below to enable the Policy Server to communicate with RSA Authentication Manager:

1. Shut down the CA SiteMinder Administrative Server, Health Monitor Service and Policy Sever.
2. Install an RSA Authentication Agent on the same machine as the SiteMinder Policy Server.
3. Use the RSA Agent's Control Center utility to perform a test authentication. After you have been authenticated, the agent will place an RSA Authentication Manager Node Secret on your computer.
4. Copy the following files from the *C:\Program Files\Common Files\RSA Shared\Auth Data* directory to the *C:\Windows\System32* directory:
    - *sdconf.rec*
    - *securid*
    - *sdstatus.12*
5. Restart the CA Servers.

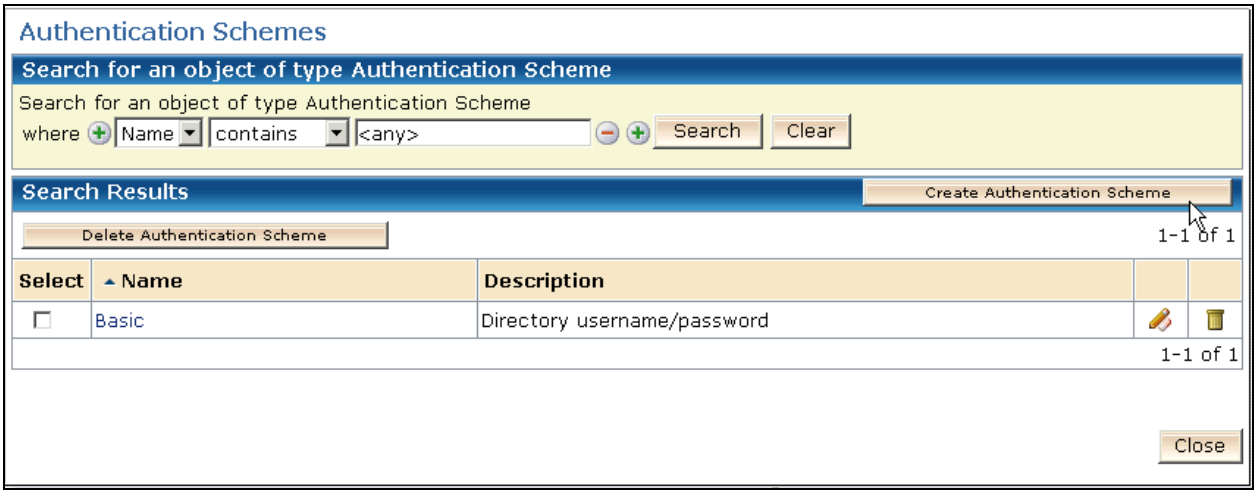
CA SiteMinder Configuration

Complete the following sections to enable RSA SecurID authentication for CA SiteMinder end-users:

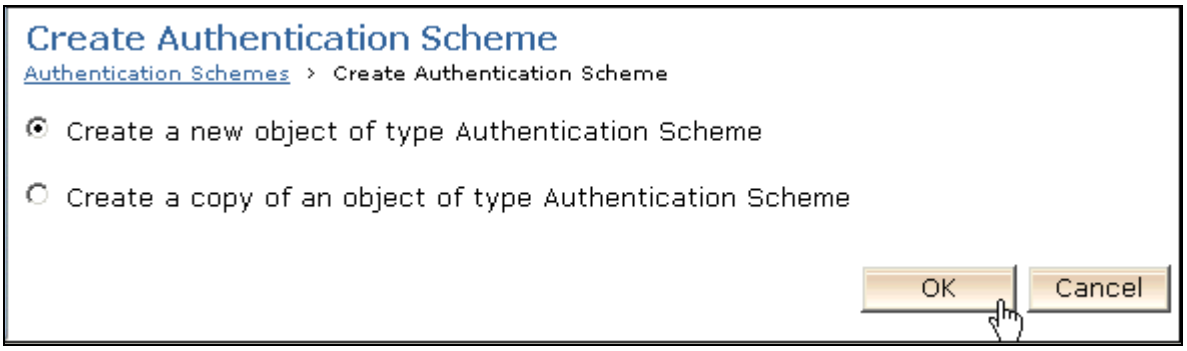
- **Create a SiteMinder Authentication Scheme for RSA SecurID Authentication**
- **Create a SiteMinder Realm for RSA SecurID Authentication**
- **Create a SiteMinder Domain Policy for RSA SecurID Authentication**

Create a SiteMinder Authentication Scheme for RSA SecurID Authentication

1. Log in to the SiteMinder Administrative UI console and click the **Infrastructure** tab.
2. Select the **Authentication → Authentication Schemes** menu item and click the **Create Authentication Scheme** button.



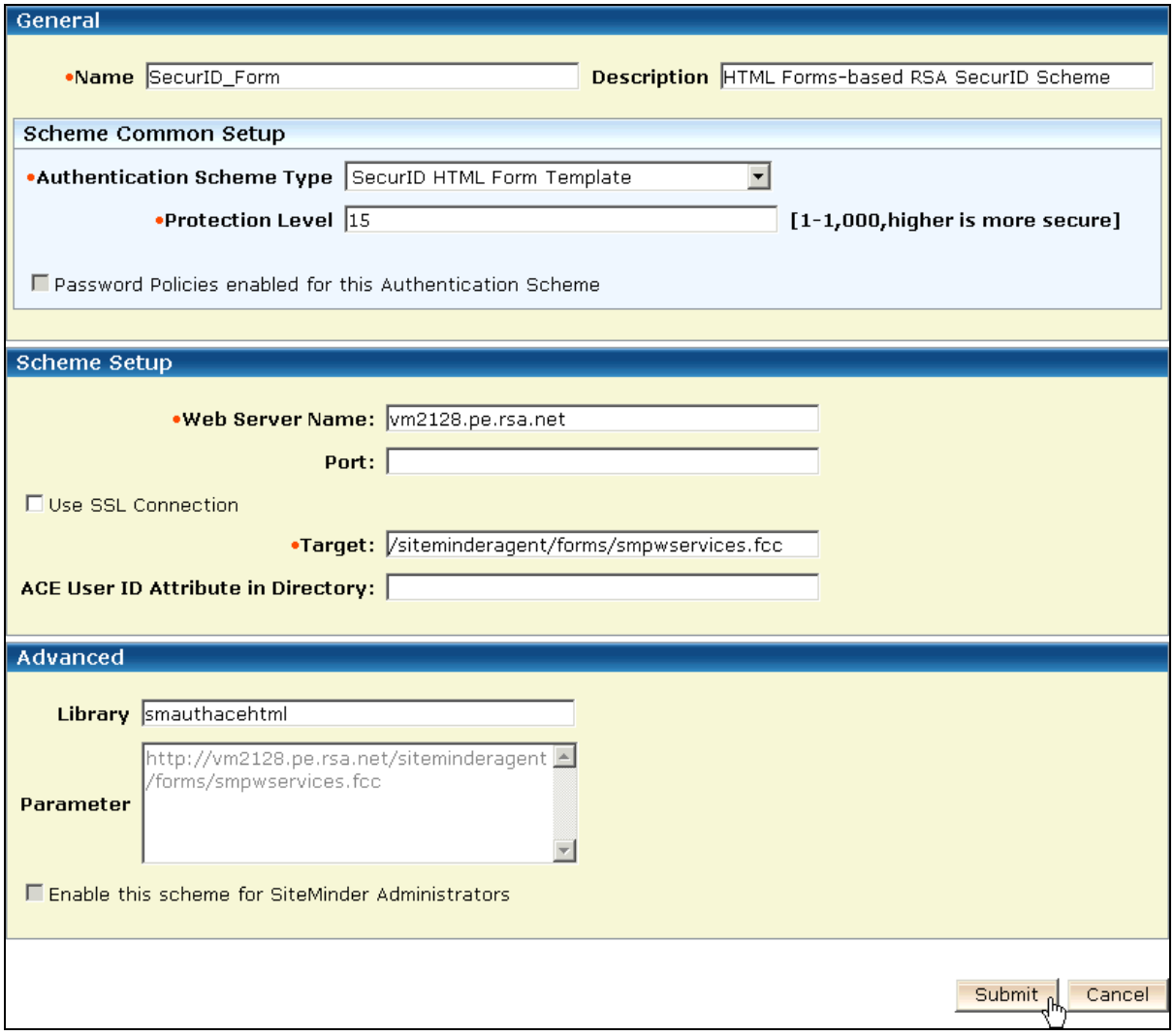
3. Select the **Create a new object of type Authentication Scheme** option and click the **OK** button.



4. Enter a unique name for your scheme in the **Name** field.
5. Select *SecurID HTML Form Template* from the **Authentication Type Style** dropdown list.

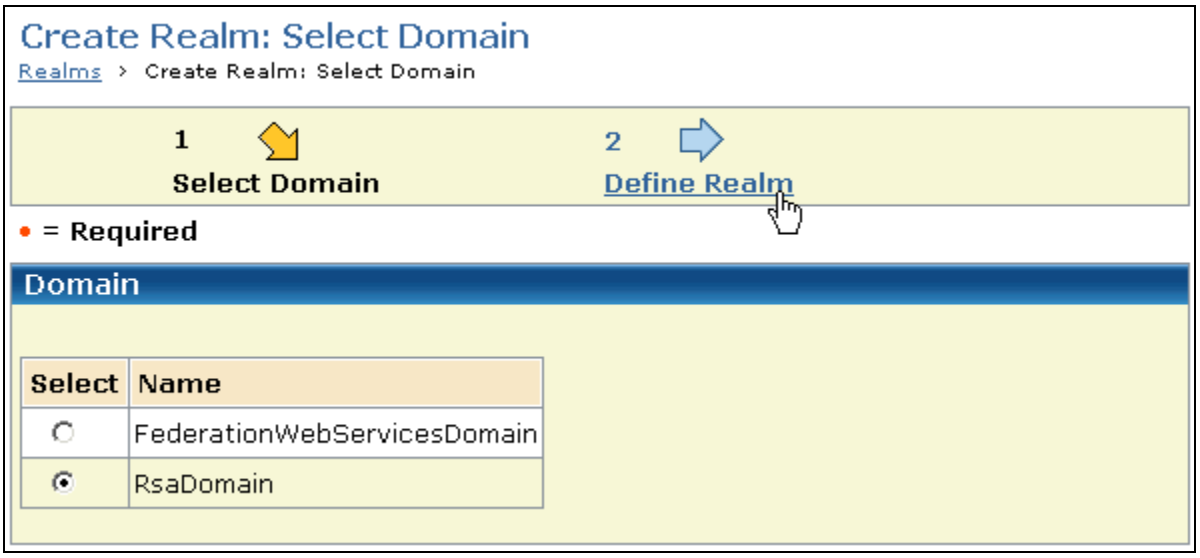
Note: CA Authentication Scheme login forms are defined in templates that contain a mixture of HTML and proprietary notation. Each of these templates has an *fcc* extension. CA provides a default RSA SecurID login template named *smpwservices.fcc*. You can either use this file or create a custom template. See the *CA Policy Server Configuration Guide* for more information.Enter the address of your login template's web server in the **Web Server Name** field and the web server's port in the **Port** field.

6. If you plan to use an SSL connection to the web server, check the **SSL** checkbox.
7. Enter the relative path to your login template in the **Target** field. The default path is */siteminderagent/forms/smpwservices.fcc*.
8. The **ACE User ID Attribute in Directory** field is used to map SiteMinder users to RSA users. If you have assigned each end user matching usernames, leave the field blank. Consult the *CA Policy Server Configuration Guide* for more information.
9. Enter *smauthacehtml* in the **Library** field. This is the name of the library that will process the authentication scheme.
10. Click the **Submit** button.

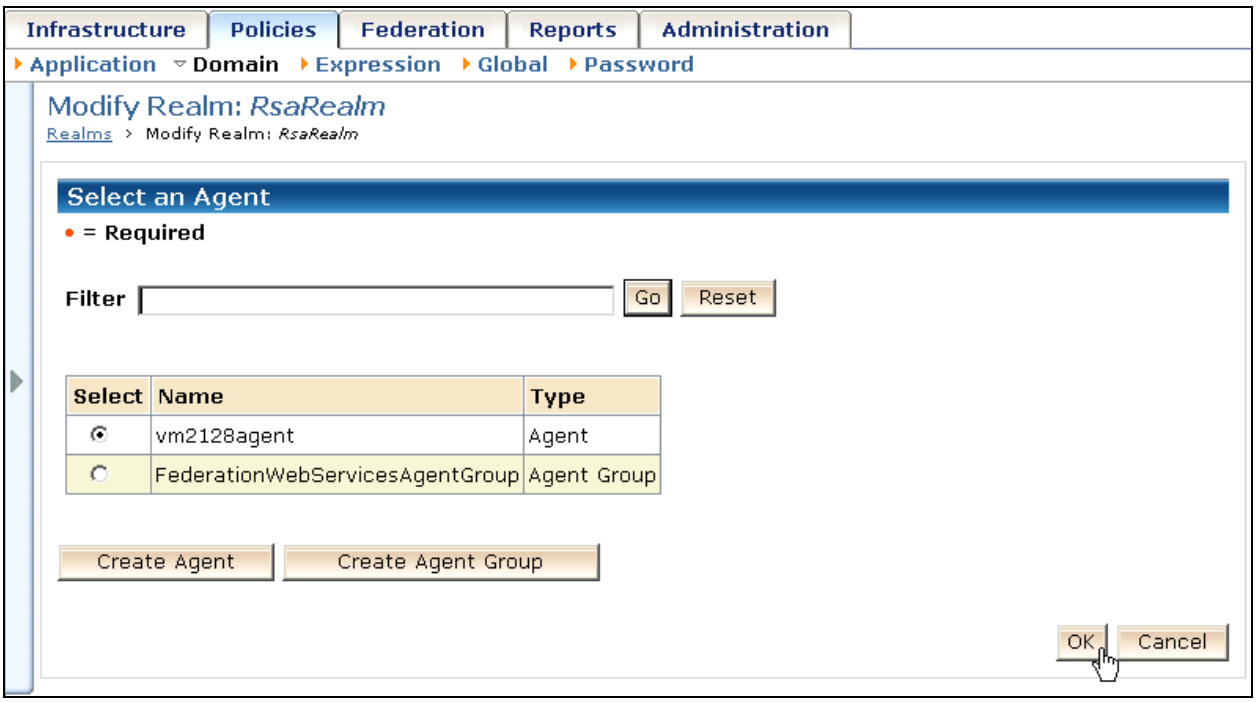


Create a SiteMinder Realm for RSA SecurID Authentication

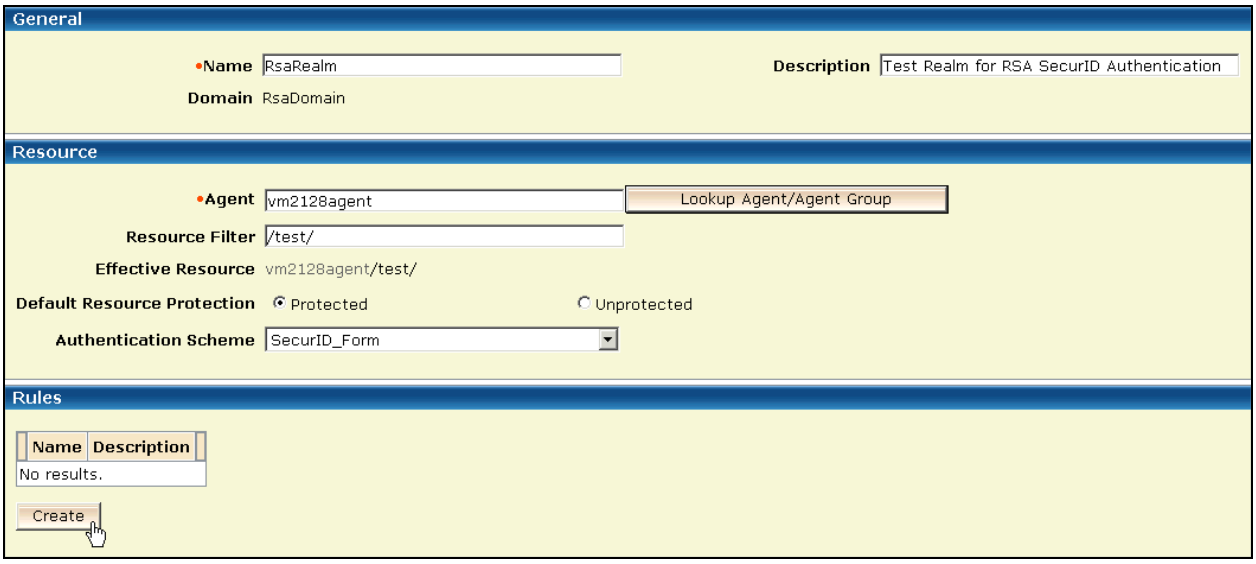
1. Click the **Policies** tab, select the **Domain → Realms** menu and click the **Create Realm** button.
2. Select a domain for your new realm and click the **Define Realm** link.



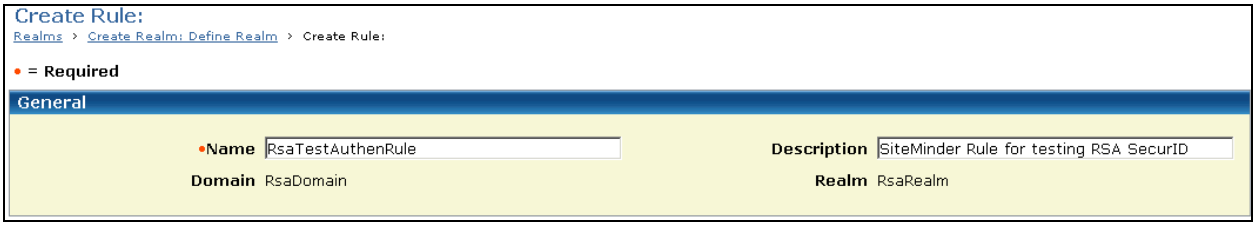
3. Enter a unique name for your realm in the **Name** field.
4. Click the **Lookup Agent** button, select the radio button for the appropriate CA web agent and click the **OK** button.



5. Your realm will protect resources in a directory on your SiteMinder Web Server Agent's host. Enter the relative name of the directory that contains these resources in the **Resource Filter** field. In the example below, all of the Realm's resources are contained in or below the *test* directory.
6. Select the **Protected** radio button.
7. Select the name of your authentication scheme from the **Authentication Scheme** dropdown list.
8. Click the **Create** button in the **Rules** section.

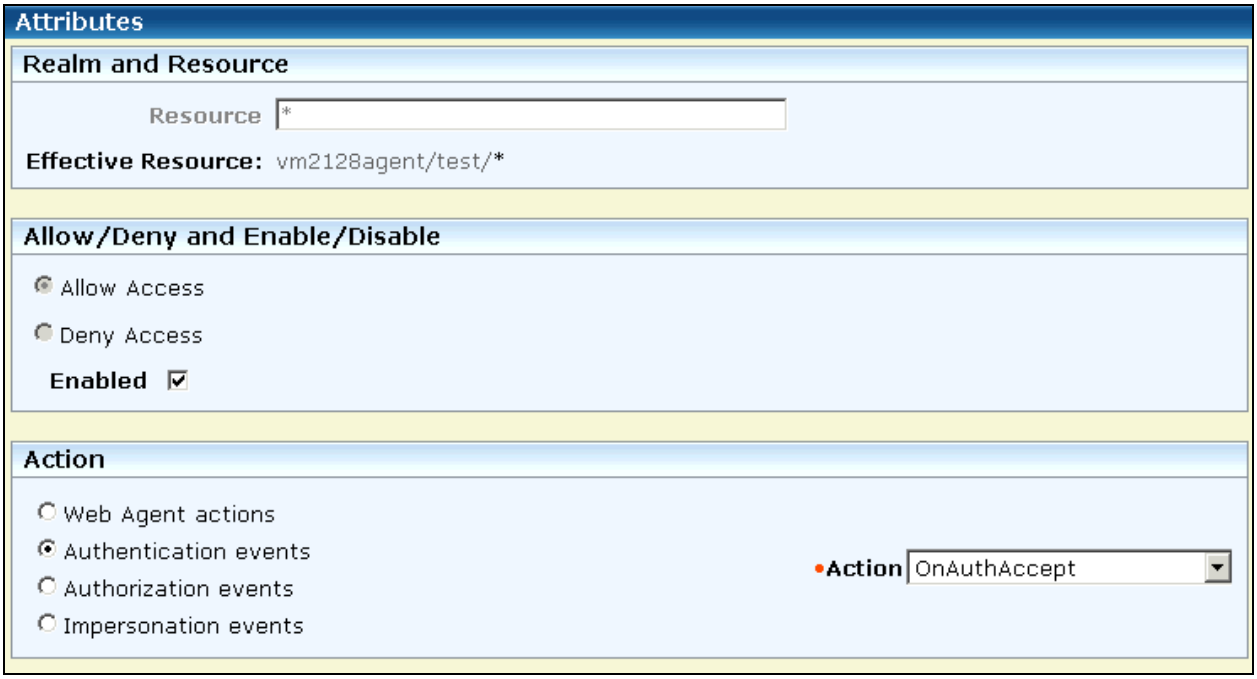


9. Enter a unique name for the rule in the **Name** field.



10. SiteMinder applies each rule you define to one or more resources based on your configuration. Enter a filter that defines these resources in the **Resource** field. The filter in the following example includes all resources below the agent's root. Consult the *CA Policy Server Configuration Guide* for information about resource filter syntax.

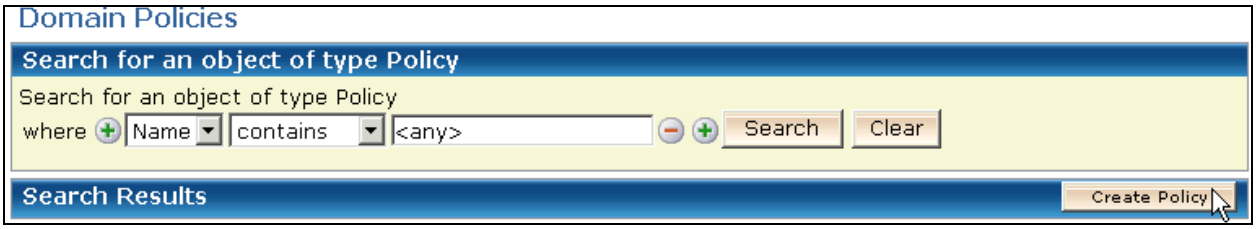
11. Define the remaining attributes for the rule based on your requirements and click the **OK** button.



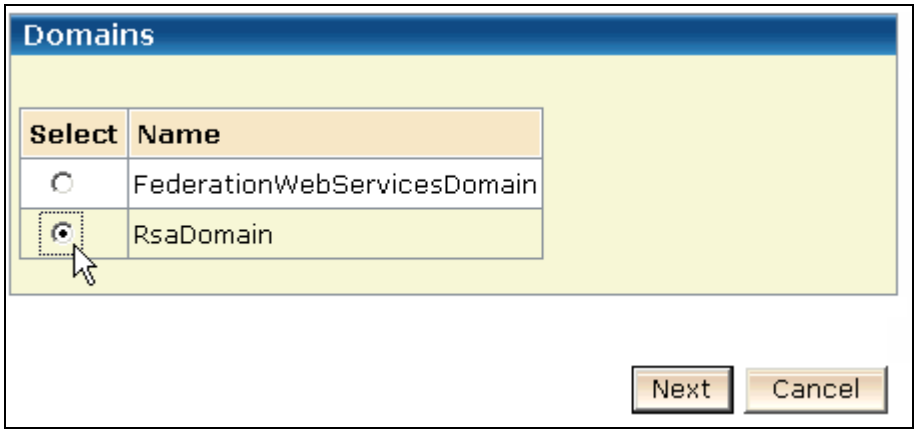
12. Repeat steps 8 through 11 for as many rules as you want to add to your realm.
13. Define any attributes in the **Advanced** section based on your requirements and click the Finish button. Consult the *CA Policy Server Configuration Guide* for information about the advanced realm parameters.

Create a SiteMinder Domain Policy for RSA SecurID Authentication

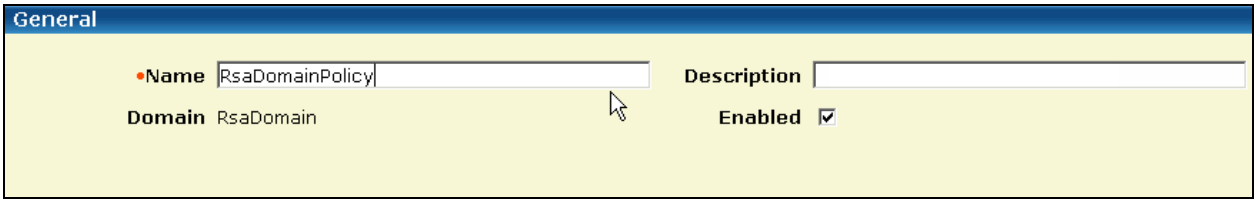
1. Click **Policies →Domain → Domain Policies** and click the **Create Policy** button.



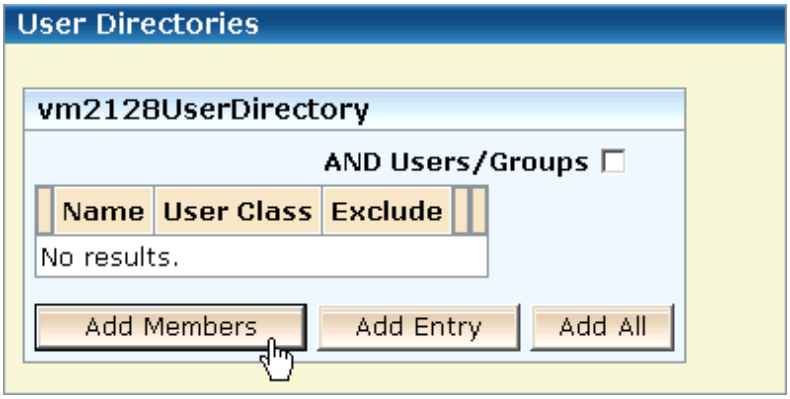
2. Select the radio button for your domain and click the **Next** button.



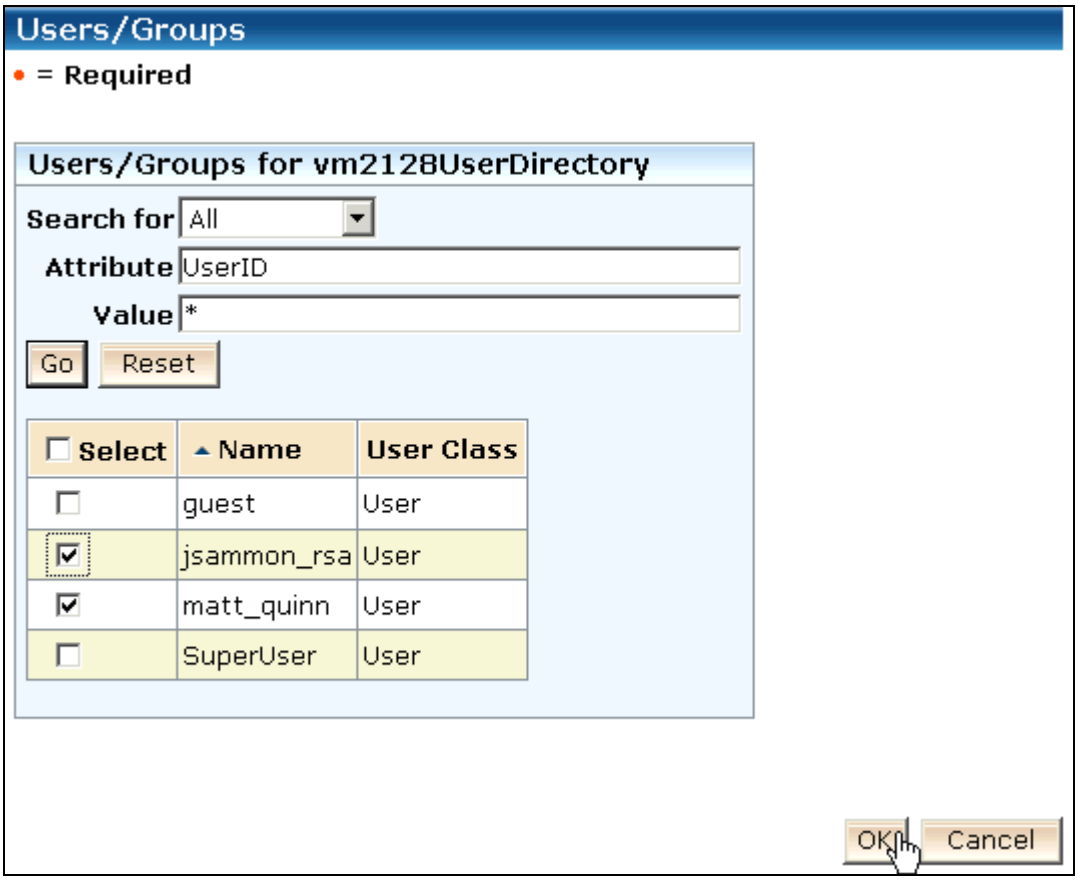
3. Enter a unique domain policy name in the **Name** field and check the **Enabled** checkbox.



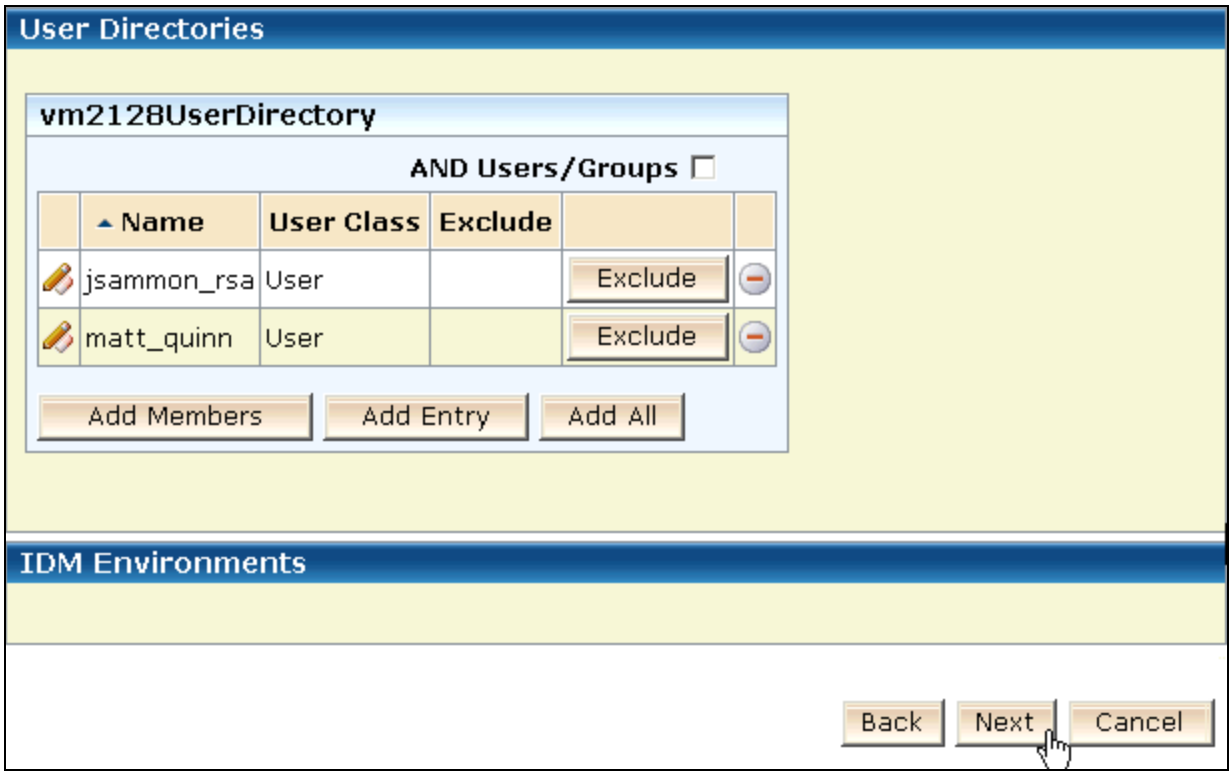
4. Define any attributes in the **Restrictions** and/or **Advanced** sections based on your requirements and click the **Next** button. Consult the *CA Policy Server Configuration Guide* for information.
5. Click the **Add Members** button in the **User Directories** section.



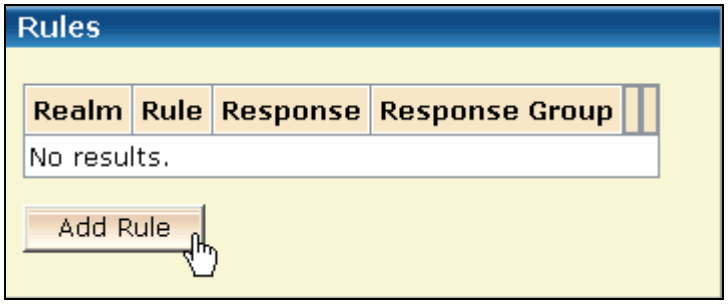
6. You will now query your backend data store for the users and/or groups you want to bind to your policy. Select *All*, *Users* or *Groups* from the **Search** for dropdown list based on your preference.
7. Enter the name of the user/group LDAP attribute or database field you want to query in the **Attribute** field. For example, you may want to base your search on the *uid* LDAP attribute.
8. Enter an expression for your query's filter in the **Value** field and click the **Go** button.
9. Check the checkbox for each user you want to bind to your policy and click the **OK** button.



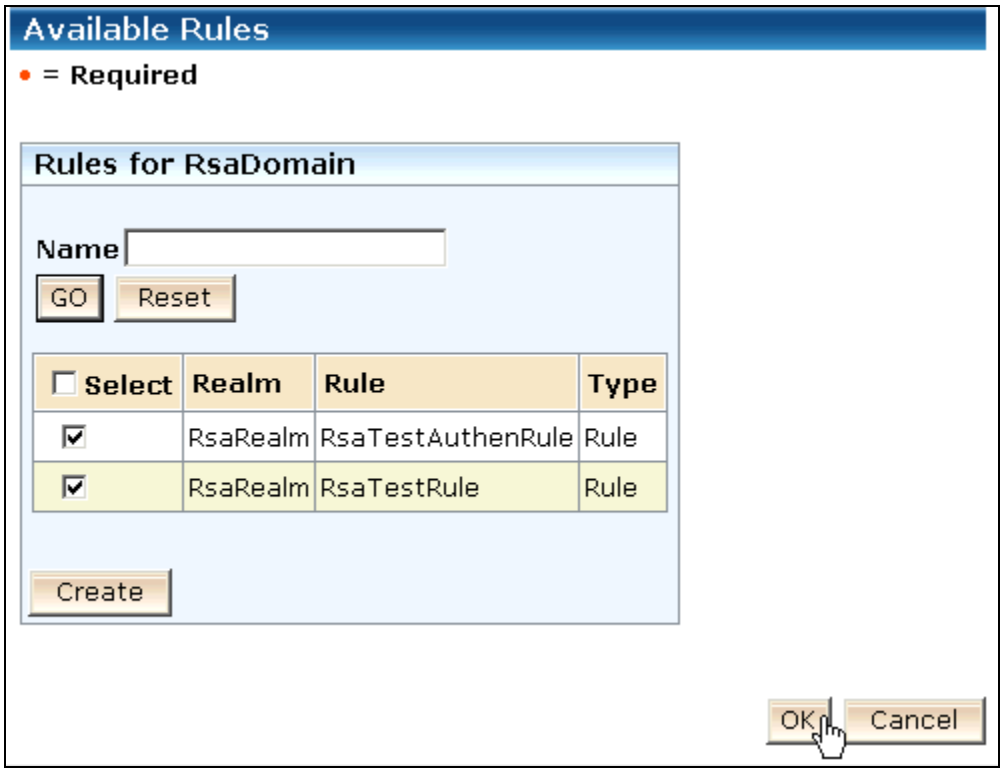
10. Click the **Next** button.



11. Click the **Add Rule** button.



12. Check the checkbox for each rule you want to add to your policy and click the **OK** button



13. Click the **Finish** button.

Risk-Based Authentication Integration

Install the CA SiteMinder RBA Script Template

In order to enable Risk-Based Authentication (RBA) for a given CA SiteMinder Web Server Agent, you must generate a Javascript file it and deploy it on the agent's web server. The script will redirect users from SiteMinder's default logon page to a custom page that allows RSA Authentication Manager to perform risk-based authentication.

The script is based on a template that ships with RSA Authentication Manager, but RSA may update the template in between releases. Follow these instructions to ensure you have the most up-to-date template.

- Download the CA SiteMinder RBA integration script template from this link:
  https://sftp.rsa.com/human.aspx?Username=partner&password=RSAS3cur3d!&arg01=859293799&arg12=downloaddirect&transaction=signon&quiet=true
- Locate the CA SiteMinder integration script template that shipped with your RSA Authentication Manager server.
- If your server doesn't have a CA SiteMinder script template, install the template you downloaded from link above. Otherwise, compare the headers of the templates and install whichever one is the newest.

Customize CA SiteMinder for Risk-Based Authentication

Once you have installed the newest template, it will be available in a dropdown list in the RSA Security Console, where you can select it to generate an RBA Javascript (am_integration.js) for your agents.

1. Log in to the RSA Security Console and chose to enable RBA for one or more of your agents.
2. Chose the primary method you want your agents to use to authenticate users (RSA SecurID or fixed passcode).
3. Select the CA SiteMinder template to generate your script and download the script to a temporary directory.
4. For each RSA Authentication Manager Agent you enabled for RBA:
   1. Log in to the agent's host machine and locate the CA SiteMinder Web Agent's default RSA SecurID login template (*smpwservices.fcc).* The template is located in the */siteminderagent/forms/* directory relative to the web agent's root.
   2. Open *smpwservices.fcc*, add the following two lines immediately before the *</body>* tag at the bottom, and save the file:

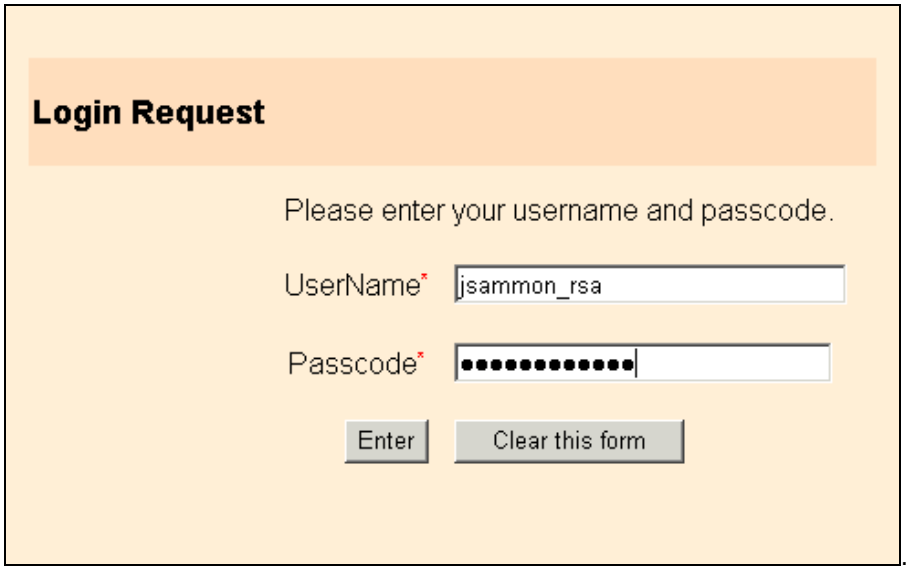
```
<script src="am_integration.js" type="text/javascript"></script>
<script>window.onload=redirectToIdP;</script>
```

Important: Create a backup of *smpwservice.fcc* before beginning to edit it and use it to undo the changes if you need to.

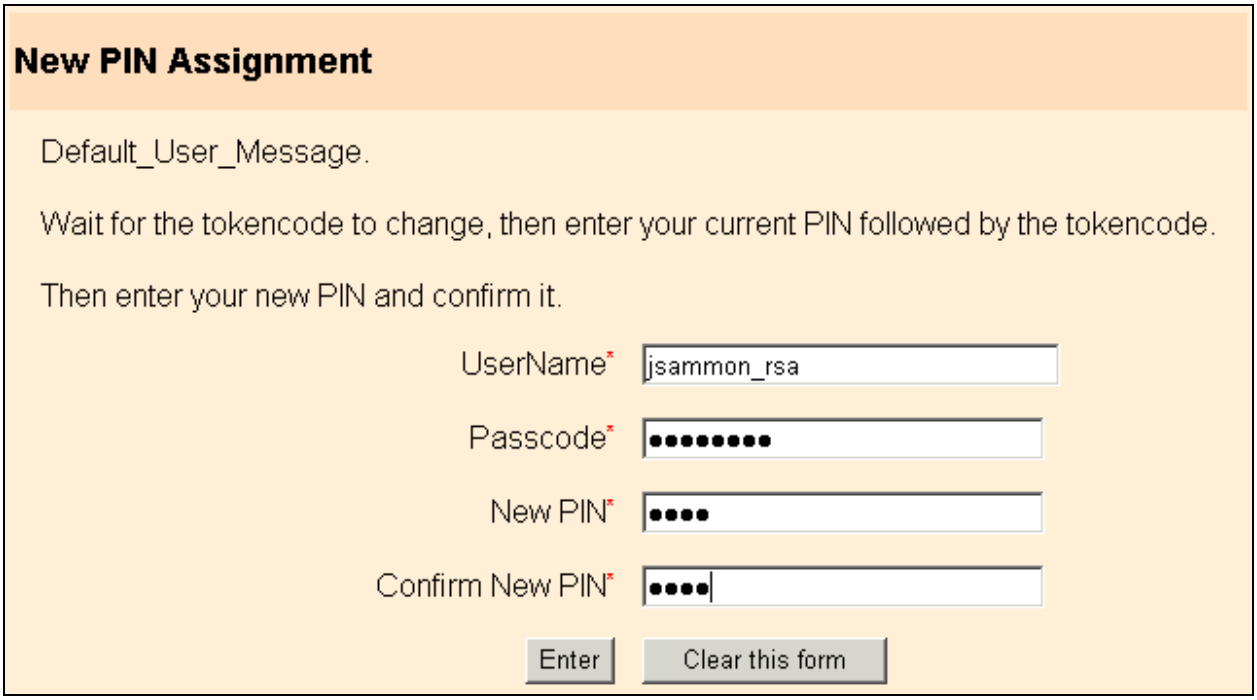
   3. Copy the Javascript you generated (*am_integration.js*) to the same directory and restart the web server.

Screenshots

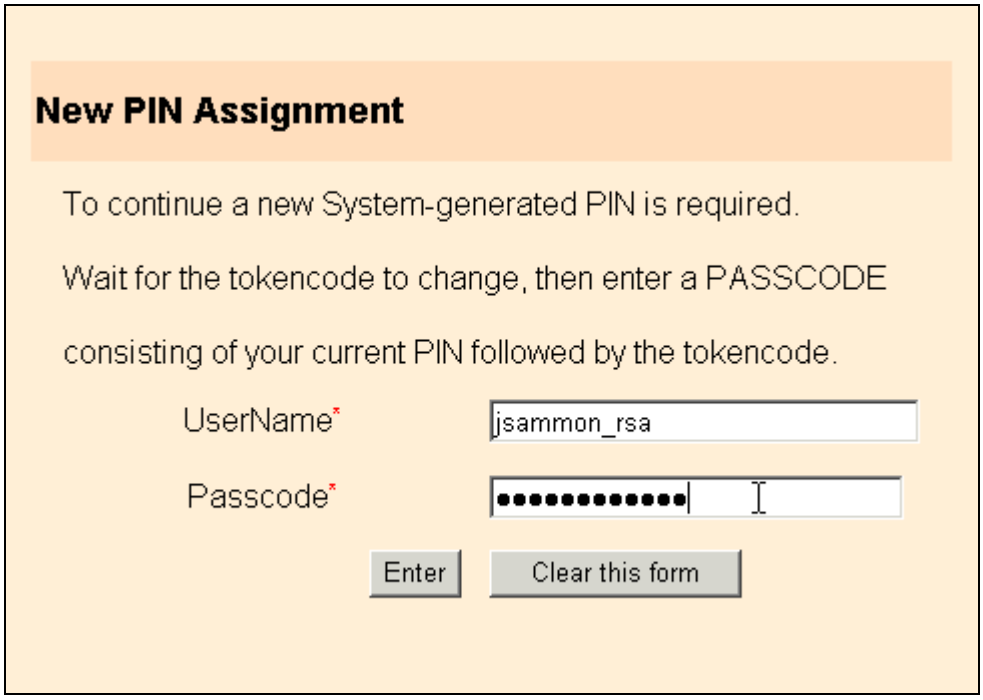
User Logon Screens



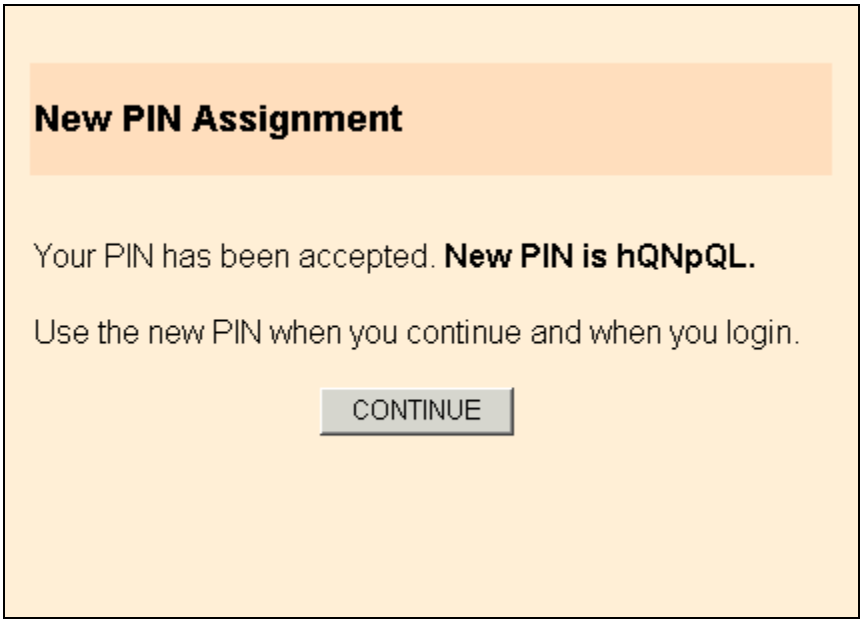
Standard Logon Prompt



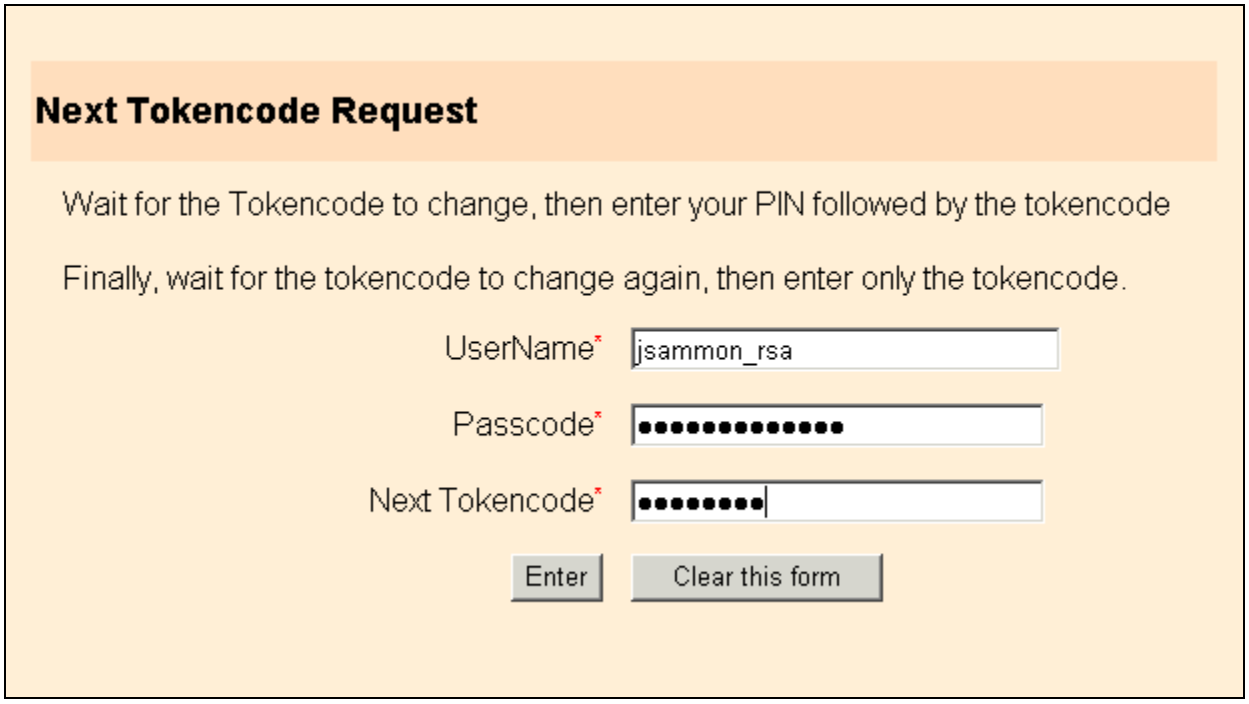
New PIN Mode Prompt



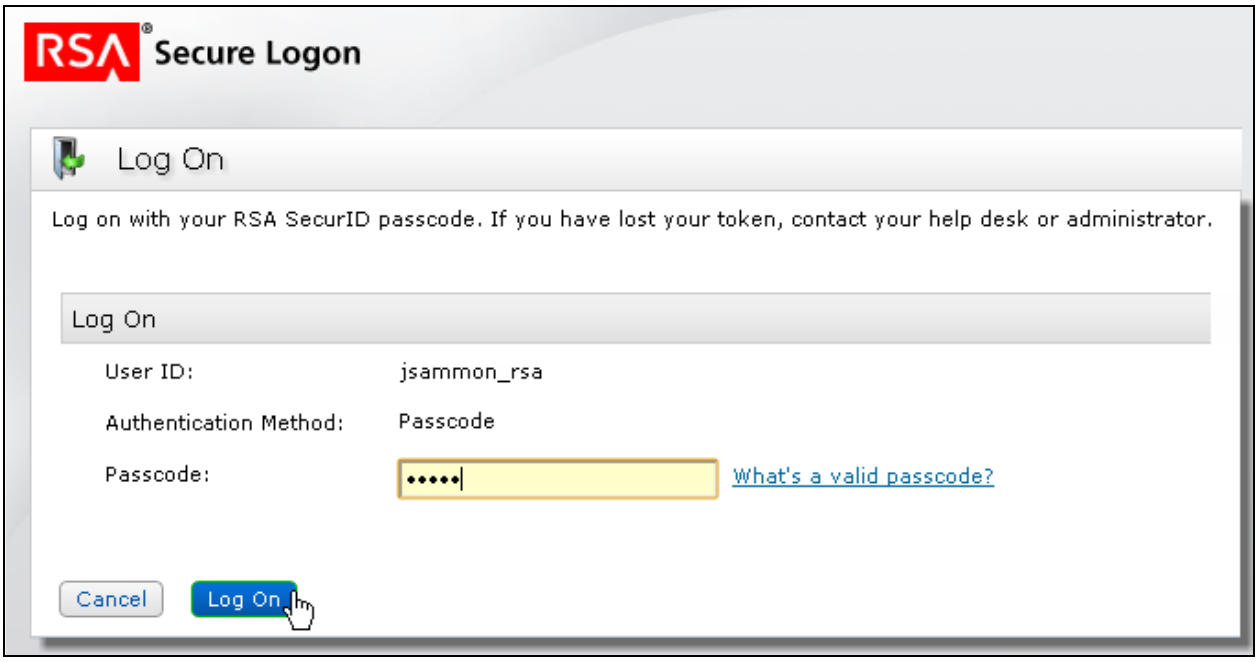
New System Generated PIN Mode Prompt



System Generated PIN Assignment Prompt



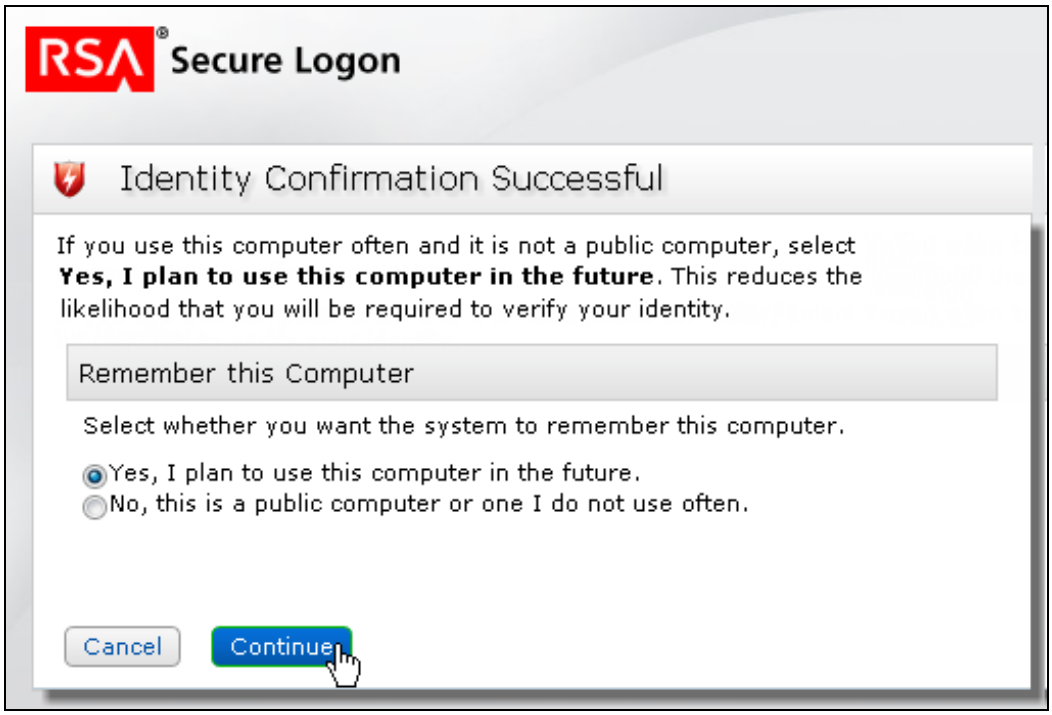
Next Tokencode Prompt



RBA Primary Authentication Prompt

RBA Create Fixed Passcode Prompt

RBA Challenge Questions Prompt



RBA Remember Computer Prompt

Certification Checklist for RSA Authentication Manager

Date Tested: 3/7/2012

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Windows 2008
RSA Authentication Agent	7.1	Windows 2008
Oracle Database	11.2.0	Windows 2008
CA SiteMinder IIS Web Agent	12.5	Windows 2008
CA SiteMinder Policy Server	12.5	Windows 2008

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	√	Force Authentication After New PIN	N/A
System Generated PIN	√	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	√	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	√	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	√	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	√	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	√	Deny Numeric PIN	N/A
Deny PIN Reuse	√	Deny PIN Reuse	N/A
Passcode			
14 Digit Passcode	√	14 Digit Passcode	N/A
4 Digit Fixed Passcode	√	4 Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	√	Next Tokencode Mode	N/A
On-Demand Authentication			
On-Demand Authentication	√	On-Demand Authentication	N/A
On-Demand New PIN	√	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	√	Failover	N/A
No RSA Authentication Manager	√	No RSA Authentication Manager	N/A

JGS

√ = Pass ✗ = Fail N/A = Not Applicable to Integration

RSA Risk-Based Authentication Functionality			
RSA Native Protocol		**RADIUS Protocol**	
Risk-Based Authentication			
Risk-Based Authentication	✓	Risk-Based Authentication	N/A
Risk-Based Authentication with SSO	✓	Risk-Based Authentication with SSO	N/A

JGS

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Appendix

Partner Integration Details	
RSA Authentication API	8.1.1
RSA User Specification	Designated Users
Display RSA Server Info	Yes (using RSA Authentication Agent)
Perform Test Authentication	Yes (using RSA Authentication Agent)
Agent Tracing	Yes (using RSA Authentication or see below)

Node Secret:

The node secret (*securid*) is stored in two locations: The RSA Authentication Agent reads the file from the *%ProgramFiles%\Common Files\RSA Shared\Auth Data* directory, and CA SiteMinder reads it from *%SystemRoot%\System32* on Windows and */var/ace* on Linux.

If you need to clear the node secret, simply delete this file. If you use the SiteMinder integration and the RSA Authentication Agent for Windows simultaneously, you must keep the two node secrets synchronized or authentication will fail.

sdconf.rec:

The *sdconf.rec* file is stored in *%SystemRoot%\System32* on Windows and */var/ace* on Linux. The RSA Authentication Agent for Windows reads *sdconf.rec from %ProgramFiles%\Common Files\RSA Shared\Auth Data*.

sdopts.rec:

This file is not used in the SiteMinder integration.

sdstatus.12:

The *sdstatus.12* file is stored in *%SystemRoot%\System32* and *%ProgramFiles%\Common Files\RSA Shared\Auth Data* on Windows and */var/ace* on Linux.

Agent Tracing (Windows):

To enable tracing on Windows, launch *regedit* from a command line, locate the *HKEY_LOCAL_MACHINE\Software\SDTI\ACECLIENT* key and create 2 DWORD values: *tracelevel* and *tracedest***.**

The value **tracelevel** specifies the verbosity and the categories of messages produced by the code. The value **tracedest** controls the output destination of the trace messages.

tracedest values:

```
SDITRACE_EVENT_LOG  0x00000001   // messages to event log
SDITRACE_CONSOLE    0x00000002   // messages to console
SDITRACE_LOGFILE    0x00000004   // messages to log file (aceclient.log)
SDITRACE_DEBUGGER   0x00000008   // messages to debugger output
SDITRACE_NOFILELINE 0x80000000   // no file and line information
```

The *SDITRACE_NOFILELINE* value can be combined with any of the other values to prevent information about the file and line number from being displayed. By default, the agent trace log file is *%SystemRoot%\aceclient.log.* To use a different log file, create a *REG_SZ:tracefile* key and set its value to the absolute path and name of the new file.

tracelevel values:

```
SDITRACEING_OFF     0x000000000  // All messages off
SDITRACEING_ON      0x000000001  // All messages marked with this level on
SDITRACEING_ENTRY   0x000000002  // All entry points use this
SDITRACEING_EXIT    0x000000004  // All function returns use this
SDITRACEING_FLOW    0x000000008  // All logic flow control use this (ifs)
SDITRACEING_GRP1    0x000000010  // Old SDITRACE macros use this (see dbglib.h)
```

To enable all tracing, set the value to *0xF*. The values can be combined to produce multiple sets of trace messages.

Note: Only use *SDITRACE_CONSOLE* for debugging as it can cause access violations during logoff.

Agent Tracing (Linux):

To enable tracing on Unix:

- Create an environment variable named *RSATRACELEVEL* and set it to a value from 0 (disable tracing) and 15(enable all tracing).
- Create an environment variable named *RSATRACEDEST* and set it to the absolute path to a debug log file.