CA Spectrum® and CA SiteMinder

Integration Guide

CA Spectrum Release 9.4 - CA SiteMinder

ca technologies

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 © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This guide references the following products:

- CA Spectrum® (CA Spectrum)
- CA SiteMinder®

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: Integration 7

Overview 7
How OneClick Is Integrated with CA SiteMinder 7
About CA Spectrum User Models 8
Configure OneClick Web Server Parameters in Policy Server 8
- Access the SiteMinder Administration Window 8
- Create a CA Spectrum OneClick Host Configuration Object 9
- Create a CA Spectrum OneClick Custom Agent Type 10
- Create a CA Spectrum OneClick Custom Agent 12
- Create a CA Spectrum OneClick Realm 12

Configure OneClick Web Server Host Registration Settings 14
- Register the OneClick Web Server with the CA SiteMinder Policy Server 14
- Configure OneClick Web Server Settings 15
- Disable or Re-enable the Integration 22

Chapter 2: Troubleshooting 23

Debugging Options 23
Disabling the Integration in the web.xml File 24
Re-Registering the OneClick Web Server 24
Specific Problems and Solutions 25
- Host Registration Fails 25
- Authentication Server (Policy Server) Cannot Be Contacted 26
- Prompted for CA Spectrum Logon Credentials When Invoking OneClick Console 26
- Cannot Access the Disable Integration Option in Single Sign-On Configuration 27
- Application Web Agents Ignore OneClick Single Sign-On Tokens 28

Index 29

Chapter 1: Integration

This section contains the following topics:

Overview (see page 7)
How OneClick Is Integrated with CA SiteMinder (see page 7)
About CA Spectrum User Models (see page 8)
Configure OneClick Web Server Parameters in Policy Server (see page 8)
Configure OneClick Web Server Host Registration Settings (see page 14)

Overview

The CA Spectrum and CA SiteMinder integration lets OneClick use CA SiteMinder Single Sign-On security management capabilities to authenticate CA Spectrum users. The integration also supports users of applications such as CA Portal and eHealth Reports that are integrated with CA Spectrum.

OneClick users experience single sign-on in the integrated application environment as follows:

- Users are not prompted for login credentials when they start the OneClick Console from the OneClick home page.
- Users logged in to the CA Portal can start the OneClick Console without having to explicitly log in to OneClick.
- Users can invoke eHealth Reports (Solaris version only) from OneClick if OneClick and eHealth have been integrated and the user is a valid CA eHealth user.

  Note: For more information, see the *CA eHealth and CA Spectrum Integration and User Guide*.

How OneClick Is Integrated with CA SiteMinder

Complete the following procedures to integrate CA Spectrum OneClick with CA SiteMinder:

1. Configure the required OneClick web server parameters (see page 8) on the SiteMinder Policy Server.
2. Register the OneClick web server (see page 14) as a trusted host with Policy Server from the OneClick Administration Pages.

More information:

Configure OneClick Web Server Parameters in Policy Server (see page 8)
Configure OneClick Web Server Host Registration Settings (see page 14)

About CA Spectrum User Models

Before users can access OneClick in a single sign-on environment, they must have corresponding CA Spectrum user models. The administrator creates a model for each user in CA Spectrum.

For more information, see the *Administrator Guide.*

Configure OneClick Web Server Parameters in Policy Server

This section describes procedures for setting up the following CA Spectrum OneClick integration components in Policy Server:

- CA Spectrum OneClick host configuration object
- CA Spectrum OneClick custom agent type
- CA Spectrum OneClick custom agent
- CA Spectrum OneClick realm

Note: See the CA SiteMinder Help if you require more information on Policy Server concepts and components referenced but not covered in detail in this section.

Access the SiteMinder Administration Window

The Administration window is the user interface to the SiteMinder Policy Server.

Follow these steps:

1. Access the Main Policy Server web page using the URL provided by a CA SiteMinder administrator.
2. Click Administer Policy Server.

   The Administration Login window opens.
3. Log on as a Policy Server administrator for the domain specified in the Main Policy Server web page address using credentials provided by the CA SiteMinder administrator.

   The CA SiteMinder Administration window opens.

Create a CA Spectrum OneClick Host Configuration Object

When you create a CA Spectrum OneClick web server host configuration object, you specify the parameters the CA Spectrum OneClick web server host uses when it connects to the SiteMinder Policy Server.

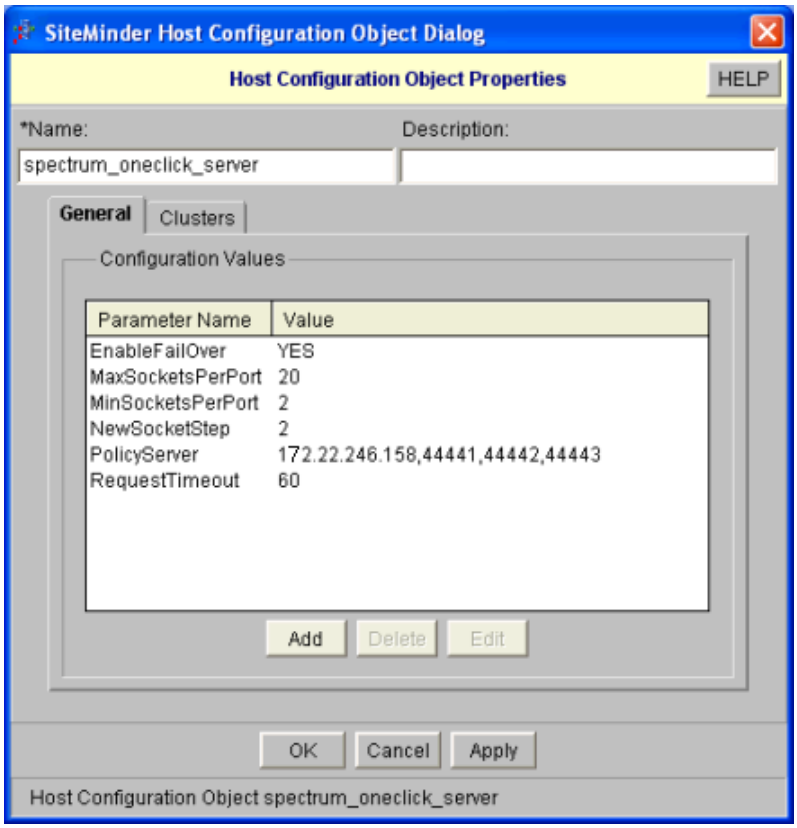
Follow these steps:

1. From the System tab, select Host Conf Objects.
2. Select the DefaultHostSettings object in the Host Conf Object list, and then select Edit, Duplicate Configuration Object.

   The SiteMinder Host Configuration Object Dialog opens.
3. Type **spectrum_oneclick_server** in the Name field.
4. Modify the Configuration Values as follows. To change a value, select the parameter and click Edit.
   - Verify that the EnableFallOver value is 'YES'.
   - Change the #PolicyServer entry (if it exists) to PolicyServer and define the correct IP address for it.

   Leave the defaults for all the other parameter values.

The configuration looks like this:



5. Click Apply.

   The new object is saved.

6. Click OK.

Create a CA Spectrum OneClick Custom Agent Type

The CA Spectrum OneClick custom agent type defines the actions that can be performed by the CA Spectrum OneClick custom agent.

Note: Verify that the View, Agent Types option is selected.

Follow these steps:

1. From the System tab, select Agent Types.
2. From the Edit menu, select Create Agent Type.

   The SiteMinder Agent Type Dialog opens.

3. Type **Spectrum OneClick Custom agent** in the Name field.

4. Define an action as follows:
   a. Click Create in the Agent Type Definition tab.

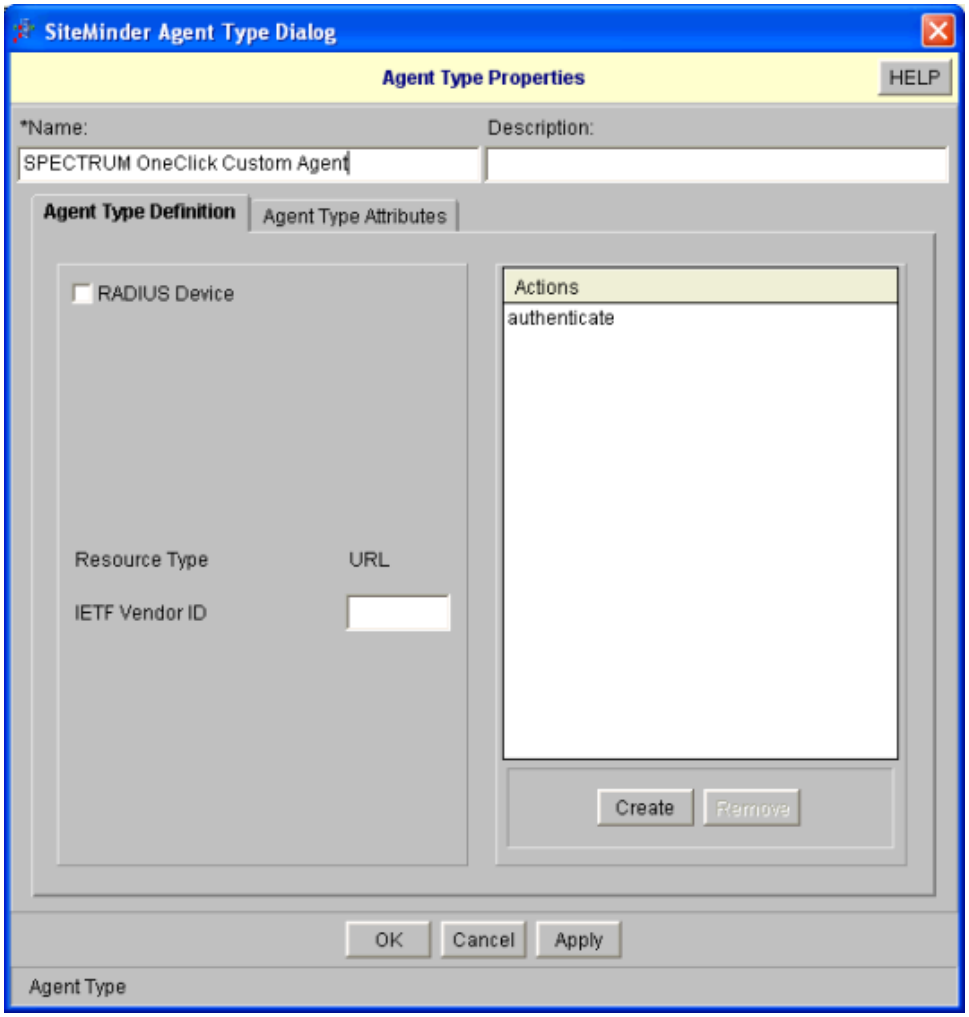
      The New Agent Action box opens.

   b. Type **authenticate**.

   c. Click OK.

      The action name appears in the Actions list.

   The configuration looks like this:



5. Click OK.

   The new agent type is now created.

Create a CA Spectrum OneClick Custom Agent

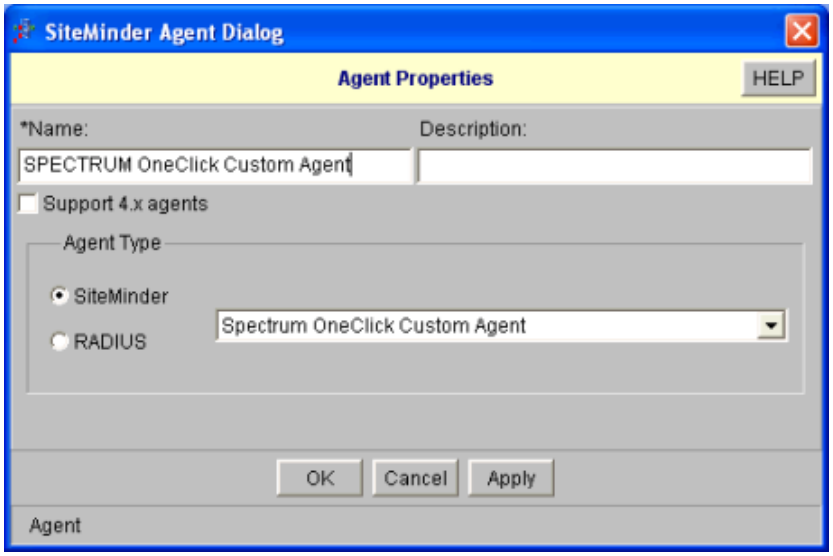
The CA Spectrum OneClick custom agent enforces the Policy Server actions on the OneClick web server.

Follow these steps:

1. From the System tab, select Agents.
2. From the Edit menu, select Create Agent.

   The SiteMinder Agent Dialog opens.
3. In the Name field, type **Spectrum OneClick Custom Agent**.
4. Verify that the 'Support 4.x agents' option is not selected.
5. Click the SiteMinder option and select 'Spectrum OneClick Custom Agent' from the list.

   The configuration looks like this:



6. Click OK.

   The new agent is now created.

Create a CA Spectrum OneClick Realm

The CA Spectrum OneClick realm specifies the resources on the OneClick web server that are protected and that require single sign-on authentication to be accessed.

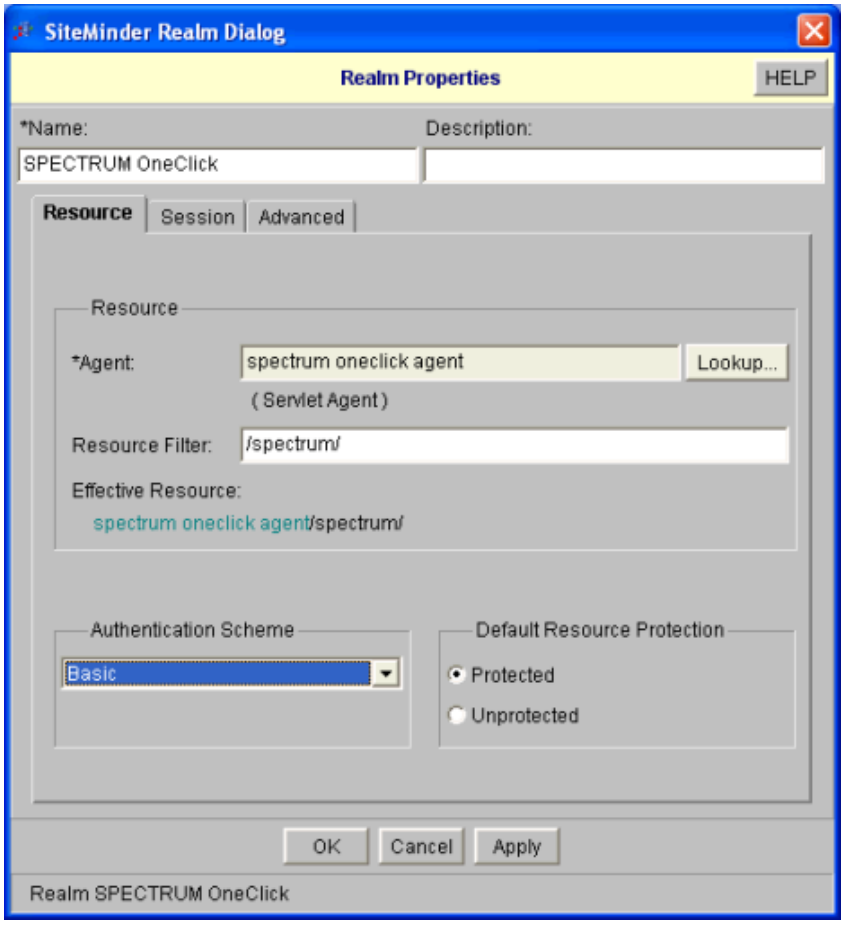
When deploying Single Sign-On for CA Spectrum OneClick and applications with which it is integrated, the CA Spectrum OneClick realm and the other application realms should be included in the same domain object. Also, the domain object user store should include users who require access to OneClick.

Follow these steps:

1. From the Domain tab, expand the icon for the domain for which you want to create the CA Spectrum OneClick realm.
2. Select Realms, Edit, Create Realm.

   The SiteMinder Realm Dialog opens.
3. Type **Spectrum OneClick** in the Name field.
4. Type **Spectrum OneClick Custom Agent** in the Agent field.
5. Type **/spectrum/** in the Resource Filter field.
6. Select the 'Protected' option in the Default Resource Protection section.

   The configuration looks like this:



7. Click OK.

   The new realm is now created.

Configure OneClick Web Server Host Registration Settings

This section includes configuration procedures for setting up log on authentication by CA SiteMinder for users who access OneClick.

Register the OneClick Web Server with the CA SiteMinder Policy Server

This section describes how to register CA Spectrum OneClick Web Server as a trusted host in the Policy Server. The term *trusted host* refers to the web server host.

When you register the web server host, initialization parameters that enable the host to connect to the Policy Server are saved to a local configuration file, SmHost.conf. Once the host connects to the Policy Server, the host uses the settings that are specified in the corresponding host configuration object in Policy Server.

Follow these steps:

1. Access the OneClick home page.
2. Click Administration.

   The Administration Pages open.
3. Click Single Sign-On Configuration.

   The Single Sign-On Configuration page opens.
4. Select the SITEMINDER option.

   The SITEMINDER Configuration form opens.
5. Specify the following registration settings in the OneClick Host Registration section:

   Policy Server IP Address

   Specifies the IP address of the Policy Server where you configured the OneClick host configuration object.

   Policy Server Port

   Specifies the Policy Server port number.

   Default: 44441

   Policy Server Admin Username

   Specifies the username of the CA SiteMinder administrator with privileges in the domain.

   Policy Server Admin Password

   Specifies the administrator password.

Trusted Host Name

Specifies the fully qualified domain name of the OneClick web server host.

Host Configuration Object

Specifies the OneClick web server host object that is configured on the Policy Server (spectrum_oneclick_server).

The OneClick host configuration should look like the following:

6. Click Register.

   Initialization parameters specified in the registration are saved to the SmHost.conf file. A new form with the "Successfully registered with the Policy Server" message opens. The form includes configuration panels where you can specify additional OneClick registration settings for the Policy Server.

Configure OneClick Web Server Settings

After you have registered the OneClick Web Server host with Policy Server, you can set additional parameters:

- In the Policy Server Settings (see page 16) panel, you can specify backup Policy Servers that have been set up for failover and the maximum amount of time (in seconds) the CA Spectrum OneClick Web Server waits before it drops a connection request from an unresponsive Policy Server.
- In the OneClick Agent Settings (see page 17) panel, specify the OneClick web server agent and cookie domain parameters. You can also instruct the web server agent to check IP addresses in cookies so that it can reject unauthorized web server requests if the IP address that is stored in a cookie does not match the IP address of the requester.

- In the Authentication Logging (see page 19) panel, you can specify whether to log authentication information to the Tomcat log file or another log file. You can also disable logging.
- In the CA Spectrum Authentication Failover (see page 20) panel, you can specify whether to allow OneClick authentication when Single Sign-On authentication fails because the Policy Server cannot be reached. This means that CA Spectrum users would be able to log on to OneClick as they normally would without single sign-on.

These settings do not take effect until you save the settings and enable the integration.

The following sections describe the configuration panels and OneClick registration settings in more detail.

Policy Server Settings

The Policy Server Settings panel is available on the OneClick Administration, Single Sign-On Configuration page in the SITEMINDER Configuration form. This form is available after you have successfully registered the OneClick Web Server host with the Policy Server. For more information, see Register the OneClick Web Server with the SiteMinder Policy Server (see page 14).

In the Policy Server Settings panel, you can specify one or more backup Policy Servers that have been configured for failover. The OneClick Web Server attempts to connect to a backup Policy Server if it detects that the primary Policy Server that is specified in the Registration form is down.

The following shows the Policy Server Settings panel:

You can also specify the timeout interval for connection requests by the OneClick web server to the Policy Server. Set an interval in the Policy Server Settings form. The OneClick web server drops the request if the Policy Server does not respond within the interval. The default interval is 60 seconds. Increase the interval if your connection requests result in frequent drops in high-data traffic or network slowdowns.

Note: The OneClick web server does not attempt to connect to a backup server after a request drop because a connection failure alone does not necessarily indicate that the primary server is down.

Follow these steps:

1. To add a backup server, enter the IP address and a port number for the backup server if it differs from the default port, 44441, and click Add.

   The backup server and port number are added to the Policy Servers box.

2. To remove a backup, select the server entry in the Policy Servers box, and click Remove.

   The backup entry is removed from the Policy Servers box.

3. To modify the Request Timeout interval, enter a new interval value.

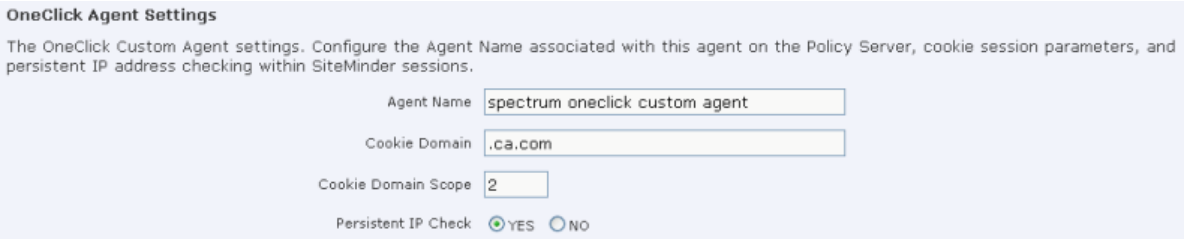
4. Specify whether the Policy Server skips validation of the session IP. Validation if the IP address of the session is changed by a reverse proxy.

Configure OneClick Agent Settings

The OneClick Agent Settings panel is available on the OneClick Administration, Single Sign-On Configuration page in the SITEMINDER Configuration form. This form is available after you have successfully registered the OneClick Web Server host with the Policy Server. For more information, see Register the OneClick Web Server with the SiteMinder Policy Server (see page 14).

In the OneClick Agent Settings panel, you can specify web agent configuration settings for this trusted host (the OneClick web server).

The following image displays the OneClick Agent Settings panel:



Follow these steps:

1. From the Single Sign-On Configuration page, navigate to the OneClick Agent Settings panel and configure the following settings:

   Agent Name

   Indicates the name of the CA Spectrum OneClick custom agent that is created in Policy Server.

   Cookie Domain

   Indicates the cookie domain for the OneClick web server agent. Use the following format for the domain value:

   `.your_company.com`

   Note: If you are trying to inter-operate between eHealth and CA Spectrum using CA EEM or CA SiteMinder, a second-level domain or greater is required for the cookie domain.

   Cookies are restricted to a certain domain level for security reasons. According to "RFC 2901" and "RFC 2965", cookies cannot be set to a top-level domain (such as .com, .org, .gov). A minimum of second-level domain is required. For more information, consult the RFC documentation.

   If a domain name ends with a two letter country code, a minimum of a third-level domain is required. A cookie that is set to a second-level domain is visible at all of its third-level domains. However, a cookie that is set to a third-level domain is not visible at its parent second-level domain or at other sub domains. If no domain name is specified when a cookie is written, the cookie domain attribute defaults to the domain name where the application resides.

   Cookie Domain Scope

   Indicates a cookie domain scope value. The scope determines the number of sections, which are separated by periods, that make up the domain name. Consider the following example:

   - Scope = 0, the most specific scope for a given host. (*Not supported in this release.*)
   - Scope = 2, .your_company.com
   - Scope = 3, your_division.your_company.com

   Note: A scope value of 1 is not allowed by the HTTP specification.

   Default: 2

Persistent IP Check

Enables (Yes) or disables (No) the agent to verify that a single sign-on session token originates from an IP address that differs from the IP address where it is created. If the agent detects a mismatch, it denies the session request.

2. Click OK.

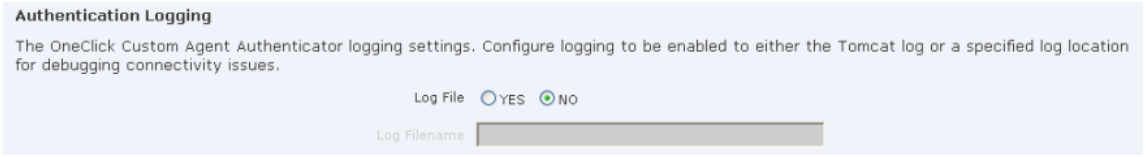
   OneClick agent settings are configured.

Configure Authentication Logging

The Authentication Logging panel is available on the OneClick Administration, Single Sign-On Configuration page in the SITEMINDER Configuration form. This form is available after you have successfully registered the OneClick Web Server host with the Policy Server. For more information, see Register the OneClick Web Server with the SiteMinder Policy Server (see page 14).

In the Authentication Logging panel, you can enable verbose logging of authentication and authorization activities for all authentication requests. By default, log files are written to the Tomcat log file (stdout.log on Windows, Catalina.out on Linux/Solaris). However, you can specify another file and location. Log files include information that can help you troubleshoot authentication and authorization problems. For example, the log indicates whether a user was authenticated properly in the Policy Server and whether a user had the appropriate role associated with a CA Spectrum user model for the OneClick application.

The following shows the Authentication Logging panel:



Note: Because of the large amount of information that is written to the log file, only enable verbose logging as required for troubleshooting purposes. Do not leave it enabled for an extended period of time.

Follow these steps:

1. To enable logging to the Tomcat log, select YES.
2. To enable logging to a specific file (not the Tomcat log), select YES and enter the full log file path and the log file name in the Log Filename box.
3. To disable logging, select NO (default).

More information:

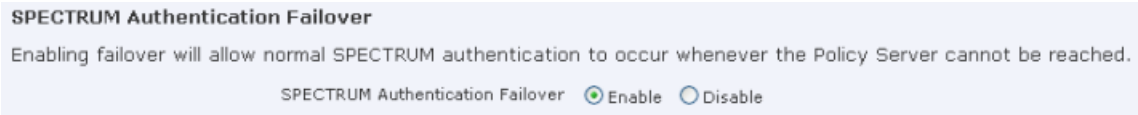
Troubleshooting (see page 23)

CA Spectrum Authentication Failover

The CA Spectrum Authentication Failover panel is available on the OneClick Administration, Single Sign-On Configuration page in the SITEMINDER Configuration form. This form is available after you have successfully registered the OneClick Web Server host with the Policy Server. For more information, see Register the OneClick Web Server with the SiteMinder Policy Server (see page 14).

In the CA Spectrum Authentication Failover panel, you can specify whether users are able to log on to OneClick as they normally would (without Single Sign-On) if the OneClick Web Server connection to the Policy Server fails. Do not enable failover if your organization prefers for personnel to access OneClick only through Single Sign-On.

The following shows the CA Spectrum Authentication Failover panel:



Note: CA Spectrum user passwords may differ from those used by Policy Server to authenticate those users.

To enable authentication failover, select Enable.

User logon requests are authenticated by CA Spectrum if Single Sign-On fails. Users who have logged on to OneClick through Single Sign-On are prompted to provide CA Spectrum logon credentials when authentication failover occurs. Conversely, when a connection to the Policy Server is established, those users are prompted for Single Sign-On logon credentials.

To disable authentication failover, select Disable (default).

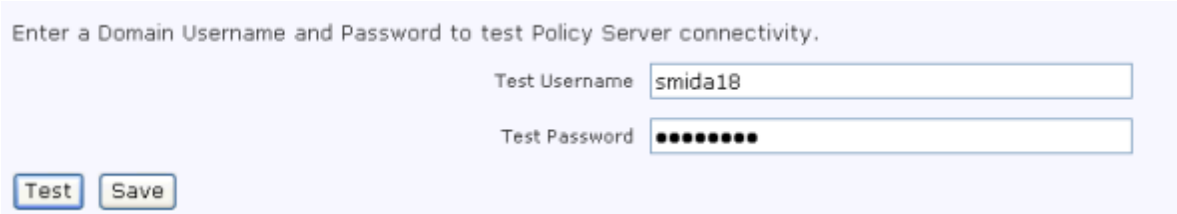
User logon requests are not authenticated by CA Spectrum if Single Sign-On fails.

Test and Save the Integration

Options to test and save the integration configuration settings are available in OneClick. In OneClick Administration, a Single Sign-On Configuration page is included in the SITEMINDER Configuration form. This form is available after you have successfully registered the OneClick Web Server host with the Policy Server. For more information, see Register the OneClick Web Server with the CA SiteMinder Policy Server (see page 14).

Execute an integration test after you have set integration parameters and before you save and enable the integration. The test determines whether you configured the connection parameters correctly and the test username and test password match an entry in the domain. If the test fails, you can reconfigure parameters and re-test. After you have successfully tested the settings, you can save them, automatically enabling the integration.

The following shows the Test and Save options at the bottom of the SITEMINDER Configuration form:



Test the integration settings from OneClick Administration.

Follow these steps:

1. Enter a username and password from the Policy Server domain user directory in the Test Username box and Test Password field. CA SiteMinder administrators manage the user directory and provide the password for Single Sign-On authentication.

   Note: The username in the Policy Server user directory must match the username created in the applications (CA Spectrum, eHealth) that the user plans to access.

2. Click Test.

   If the test is successful, the following message appears:

   “Successfully established connection with the Policy Server”

You can also save the integration settings.

Follow these steps:

1. Click Save to save the integration settings.

   You are prompted to restart Tomcat.

2. Click OK to restart Tomcat to apply the configuration.

   SiteMinder single sign-on integration in OneClick is enabled.

More information:

Troubleshooting (see page 23)

Disable or Re-enable the Integration

When you initially configure the CA SiteMinder integration settings, you automatically enable the integration upon saving. You can also disable and re-enable the integration if necessary. When you disable the integration, users are authenticated by the integrated applications that they access from OneClick.

Disable the CA SiteMinder integration on the Single Sign-On Configuration page in OneClick Administration.

Follow these steps:

1. Select 'No Single Sign-On' and click Save.

   You are prompted to restart Tomcat.

2. Click OK to restart Tomcat and disable the CA SiteMinder integration.

When the integration is disabled, you can re-enable it.

Follow these steps:

1. On the OneClick Administration, Single Sign-On Configuration page, select the SITEMINDER option.

   The SITEMINDER Configuration form opens.

2. Verify that the existing settings are correct and click Save.

   You are prompted to restart Tomcat.

3. Click OK to restart Tomcat and apply the CA SiteMinder integration configuration.

Chapter 2: Troubleshooting

This section provides solutions to problems you may encounter with the integration. If you cannot find a solution in this section to your particular problem or you need additional assistance, contact Technical Support.

This section contains the following topics:

Debugging Options (see page 23)
Disabling the Integration in the web.xml File (see page 24)
Re-Registering the OneClick Web Server (see page 24)
Specific Problems and Solutions (see page 25)

Debugging Options

OneClick provides multiple debugging options that can help you pinpoint problems with the integration.

- Users cannot log on to the OneClick home page.

  You can enable logging of authentication activities to the Tomcat log (stdout.log on Windows, catalina.out on Linux/Solaris) using the Authentication Logging option in Single Sign-On Configuration. Authentication logging indicates whether Policy Server is denying a user access to CA Spectrum OneClick or if the user role is not being retrieved from CA Spectrum.

- The OneClick web server cannot connect to Policy Server during single sign-on configuration.

  You can enable logging of information about integration parameters to the Tomcat log (stdout.log on Windows, catalina.out on Linux/Solaris) by enabling the Web Server Debug Page (Runtime)/Single Sign-On Integration option available from the Debugging link on the Administration page.

- Particular users cannot access the OneClick Console from the OneClick home page without being prompted for credentials.

  You can enable the Debug Console for Single Sign-On in the OneClick Console. It provides information about single sign-on token recognition. You can also enable this option directly in the oneclick.jnlp file.

More information:

Configure Authentication Logging (see page 19)
Prompted for CA Spectrum Logon Credentials When Invoking OneClick Console (see page 26)

Disabling the Integration in the web.xml File

In some troubleshooting scenarios where you cannot access Single Sign-On Configuration from the Administration link in the OneClick home page, you can disable the integration. Disable the integration in the web.xml file.

Follow these steps:

1. Stop CA Spectrum OneClick Tomcat.
2. Open the *$SPECROOT*/tomcat/webapps/spectrum/WEB-INF/web.xml file with a text editor.
3. Find the following element:

   ```
   <auth-method>EXTERNALSSO</auth-method>
   ```

4. Change the element content as follows:

   ```
   <auth-method>BASIC</auth-method>
   ```

5. Restart Tomcat.

   The integration is disabled.

Re-Registering the OneClick Web Server

In some troubleshooting scenarios (current registration is invalid, for example), you may have to remove the current registration and re-register the OneClick web server with the CA SiteMinder Policy Server.

Follow these steps:

1. Stop Tomcat.
2. Remove the Trusted Host Name for the server from the Policy Server.

   Note: For more information, see the Policy Server Help.

3. Remove the *$SPECROOT*/custom/sso directory.
4. Specify CA Spectrum OneClick Authentication in the web.xml file.
5. Restart Tomcat.

   Register the web server.

More information:

Disabling the Integration in the web.xml File (see page 24)
Configure OneClick Web Server Host Registration Settings (see page 14)

Specific Problems and Solutions

This section describes specific problems with CA Spectrum SiteMinder integration and recommended procedures for solving the problems.

Host Registration Fails

Valid on Linux, Solaris, and Windows

Symptom:

When you test the registration, an error message indicates that the OneClick Web Server was unable to connect to the Policy Server.

When you test the registration, an error message indicates that the OneClick Web Server was able to connect to the Policy Server, but the login credentials were invalid.

Solution:

If you received an “Invalid credentials” message, make sure the username and the password you specified in Single Sign-on Configuration are correctly configured in CA SiteMinder. Consult the SiteMinder/Policy Server administrator for assistance.

If you received an “Unable to connect” message, verify that the Policy Server is up and running and then check settings in Single Sign-on Configuration and Policy Server.

Single Sign-on Configuration:

- Verify that the Policy Server IP Address and Policy Server Port settings are correct.
- Verify that the Policy Server Admin Username and Policy Server Admin Password settings are correct. Also verify that the credentials provide administrative privileges.

Policy Server:

- Verify that the CA Spectrum OneClick host configuration object has been correctly created on the Policy Server.
- Verify that the name you specified in Single Sign-On Configuration for the Trusted Host Name setting is not a duplicate of a name that is already included as a Trusted Host in the Policy Server. If it is a duplicate, use another name or delete the name in Policy Server and retry the registration.

Authentication Server (Policy Server) Cannot Be Contacted

Valid on Linux, Solaris, and Windows

Symptom:

An error message states that the authentication server cannot be contacted when a user attempts to invoke OneClick Console.

Solution:

- Verify that the Policy Server is up and running.
- If the message mentions that the user failed to authorize, do the following:
  - On the Single Sign-On Configuration page, set Log File to “YES” and Save.
  - Look at the Tomcat log after the user attempts to log on. The log indicates whether the Policy Server is denying the user or if the user role is not being retrieved from CA Spectrum.

Prompted for CA Spectrum Logon Credentials When Invoking OneClick Console

Valid on Linux, Solaris, and Windows

Symptom:

Even though the integration is enabled, the user is prompted for a CA Spectrum username and password when attempting to start the OneClick Console from the OneClick home page.

Solution:

An error might have occurred in the communication of Single Sign-On parameters to OneClick from the web server. To display how Single Sign-On information is being transferred, enable OneClick to display the java debug console.

Follow these steps:

1. Edit the JNLP file (located at *$SPECROOT*/tomcat/webapps/spectrum/oneclick.jnlp).
2. Find the following line:

   ```
   <!--<argument>-debug Poller=on</argument> -->
   ```

3. Add the following line below it:

   ```
   <argument>-debug SSOConsoleDebug=on</argument>
   ```

4. Launch into the OneClick Console with the java debug console displayed.

   If you detect that the -ssoToken parameter is not being passed or it does not have a value associated with it, there is a problem with how your Single Sign-On cookies are being written. Make sure your cookie settings (located in the OneClick Agent Settings area of the Single Sign-On Configuration administration page) coincide with how you are accessing your OneClick web server.

Example: Incorrect Cookie Setting Causes Authentication Problem

The following is an example of an incorrect cookie setting that would produce the authentication problem:

- In the OneClick Agent Settings page, the cookie domain is set to ".ca.com" and the cookie scope is set to "2". This means that cookies will be written to.ca.com in the browser.
- You access your web server using http://someuser/spectrum in your URL. This violates the cookie settings because "someuser" is out of scope with the.ca.com domain. Instead, you should use http://someuser.ca.com/spectrum to access your web server.

Cannot Access the Disable Integration Option in Single Sign-On Configuration

Valid on Linux, Solaris, and Windows

Symptom:

You cannot access the Single Sign-On Configuration page and disable the integration.

Solution:

The OneClick access authorization method is specified in the web.xml file. You can disable the integration (and restore standard CA Spectrum login access) by editing the <auth-method> element in the file.

More information:

Disabling the Integration in the web.xml File (see page 24)

Application Web Agents Ignore OneClick Single Sign-On Tokens

The OneClick implementation of CA SiteMinder uses its own customized agent, rather than an installed web server agent, to communicate with the SiteMinder policy server. If you are sharing single sign-on tokens between OneClick and installed web agents of other applications, you may need to modify the agent configuration of each installed web agent to recognize, or not ignore, OneClick agent tokens.

Set the following web agent parameter from NO to YES for the other applications:

```
AcceptTPCookie=YES
```

Index

A

Administration Pages, OneClick home page • 14
agent • 17
authentication failover, enabling to CA Spectrum • 20
authentication logging, enabling • 19
authentication server, cannot contact • 25

B

backup authentication servers, specifying • 16

C

CA Spectrum logon credentials, incorrectly prompted for • 26
CA Spectrum OneClick custom agent • 12
CA Spectrum OneClick host configuration object • 9
CA Spectrum OneClick realm • 12
CA Spectrum user models • 8
configuring parameters for in Policy Server • 8
contacting technical support • 3
cookie domain • 17
cookie domain scope • 17
custom agent • 12, 17
customer support, contacting • 3

D

debugging • 23
disable integration • 21

E

enable integration • 21

F

failover, authentication server • 16

H

Host Conf Objects • 9
host configuration object • 9
host configuration object dialog box • 9

I

initialization parameters in SmHost.conf file • 14
integration
  disable from configuration panel • 21
  disabling in the web.xml file • 24
  enable • 21
  procedure overview • 7
  process overview • 7
  test • 21
invalid credentials, message • 25

J

java debug console • 26

L

logging, authentication data • 19

O

OneClick custom agent type • 10
OneClick token, recognition of by application web • 28
OneClick web server
  configuring parameters for in Policy Server • 8
  host as a trusted host • 14
  register as a trusted host • 14
oneclick.jnlp • 26

P

persistent IP check • 17
Policy Server
  configure OneClick web server parameters • 8
  failover backup servers • 16

R

realm • 12
registration
  re-registering • 24
  test failure • 25
  trsuted host • 14
request timeout interval • 16
re-registering a registration • 24

S

SiteMinder Administration window, accessing • 8
SiteMinder Agent dialog • 12
SiteMinder Agent Type dialog • 10
SiteMinder Realm dialog box • 12

sso directory • 24
support, contacting • 3

T

technical support, contacting • 3
test, the integration • 21
timeout, for connection requests • 16
tomcat log • 19
troubleshooting debugging options • 23
trusted host • 14

U

unable to connect, message • 25
user models, CA Spectrum • 8

W

web agent configuration • 17
Web agents ignoring OneClick token, resolving • 28
web.xml • 24