

How to deploy the SiteMinder Test Tool On your workstation

smtest.exe (MS Windows x86 binary)

Alan Baugher
CA Sr. Principal Architect
Nov 2015

How to run smtest on command line?

<http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec547520.aspx>

Smtest tool does not work (dependency on ETPKI library)

<http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec1437596.aspx>

Summary

<http://www.ca.com/us/support/ca-support-online/product-content/status/release-notes/using-the-siteminder-test-tool-sm-test.aspx?id={6093E028-3913-419D-9C0F-7215D8FE5781}>

Challenge(s): Limited Info About SmTest Tool

← [https://support.ca.com/cadocs/0/CA SiteMinder 12 52-ENU/Bookshelf_Files/search.html?zoom_query=smtest&zoom_per_page=10&zoom_and=0&zoom_sort=0](https://support.ca.com/cadocs/0/CA%20SiteMinder%2012%2052-ENU/Bookshelf_Files/search.html?zoom_query=smtest&zoom_per_page=10&zoom_and=0&zoom_sort=0)

CA SiteMinder® 12.52

[Search Tips](#)

Enter search term Results per page: ▼

Match: ☒ any search words ☐ all search words

Search results for: smtest

2 results found.

- [1. Configure Your Test Environment Agent](#)
Describes how to configure the agent that the Test Tool simulates during a test.
Terms matched: 1 - Score: 42 - 24 Dec 2013 - URL: <HTML/idoocs/346814.html>
- [2. Defects Fixed in 12.51](#)
Release Notes SDK Release Notes Defects Fixed in 12.51 Defects Fixed in 12.51 This section contains the following topics: Incorrect Values in smre...
Terms matched: 1 - Score: 27 - 24 Dec 2013 - URL: <HTML/idoocs/2155760.html>

smtest Tool Errors when Run from the bin64 Directory (CQ162346)

Valid on Windows 2008

Symptom:
I installed the test tool and saw the following error message when I tried to run it from the bin64 directory:
`libetpki2.dll not found`

Solution:
This issue is fixed.
STAR Issue # 20994844:01

smtest.exe not observed in SDK bin64 folder

https://support.ca.com/cadocs/0/CA%20SiteMinder%2012%2052-ENU/Bookshelf_Files/HTML/idoocs/index.htm?toc.htm?346814.html?zoom_highlight=smtest

Use “test tool” as search criteria in SSO Bookshelf

Search results for: Test Tool

35 results found containing all search terms.

4 pages of results.

1. [Configure Your Test Environment Agent](#)

Describes how to configure the agent that the Test Tool simulates during a test.

Terms matched: 2 - Score: 850 - 24 Dec 2013 - URL: HTML/idocs/346814.html

2. [Run a Functionality Test](#)

Describes how run the Test Tool to test the functionality of policies in a simulated real-world environment.

Terms matched: 2 - Score: 676 - 24 Dec 2013 - URL: HTML/idocs/347283.html

3. [Run a Stress Test](#)

Describes how to use the Test Tool to test performance when multiple agents communicate with the Policy Server simultaneously or a single agent com...

Terms matched: 2 - Score: 615 - 24 Dec 2013 - URL: HTML/idocs/347364.html

4. [Test Tool Overview](#)

Introduces the SiteMinder Test Tool, a utility that simulates the interaction between Agents and Policy Servers to test your SiteMinder configurat...

Terms matched: 2 - Score: 513 - 24 Dec 2013 - URL: HTML/idocs/347482.html

5. [Certificate-based Authentication Tests](#)

Describes how to use the Test Tool to simulate certificate-based user authentication and authorization.

Terms matched: 2 - Score: 378 - 24 Dec 2013 - URL: HTML/idocs/345879.html

6. [SiteMinder Test Tool](#)

Contains links to topics related to the SiteMinder Test Tool.

Terms matched: 2 - Score: 279 - 24 Dec 2013 - URL: HTML/idocs/347394.html

7. [Perform a Regression Test by Playing Back a Test Recorded in a Command Script File](#)

Describes how to use play back a recorded Test Tool test to determine whether changes made to SiteMinder, such as upgrading the policy store or im...

Terms matched: 2 - Score: 247 - 24 Dec 2013 - URL: HTML/idocs/2148781.html

8. [SDK Samples](#)

Describes the sample programs and where they are installed. Describes the Test Tool, lists the additional documents for the SDK, and provides a di...

Terms matched: 2 - Score: 216 - 24 Dec 2013 - URL: HTML/idocs/243623.html

9. [Measure CA SiteMinder® Performance](#)

Provides a list of tools to help you identify issues related to network data, performance bottlenecks, the interaction between a Policy Server and...

Terms matched: 2 - Score: 180 - 24 Dec 2013 - URL: HTML/idocs/827010.html

10. [Policy Server Tools](#)

Contains instructions, syntax, and parameters from command-line Policy Server tools

Terms matched: 2 - Score: 165 - 24 Dec 2013 - URL: HTML/idocs/242588.html

[1](#) [2](#) [3](#) [4](#) [Next page](#)

- Additional Information under “test tool” within SSO (SM) Bookshelf.
- The first eight (8) links have the majority of information.
- UNIX/Linux information appears to be older references; as the tool is not observed on any SMPS installation for RHEL Linux.

[Start the Test Tool on UNIX](#)

Start the Test Tool to test Policy Server functionality.

Follow these steps:

1. Open a Command Window and navigate to `policy_server_home/bin`.

2. Type the following command:

```
./smtest
```

Note: To run the Test Tool on UNIX, the X display server must be running. If required, enable the display by entering the following in a Command Window:

```
export DISPLAY=n.n.n.n:0.0
```

```
n.n.n.n
```

Specifies the IP address of the Policy Server host system.

[Red Hat Enterprise Linux AS Requires Korn Shell \(28782\)](#)

A Policy Server installed on Red Hat AS requires the Korn shell. If you do not install a Korn shell on Red Hat AS, you cannot execute the commands that control the Policy Server from a command line, such as start-all and stop-all.

[Excluded Features on Red Hat Enterprise Linux AS](#)

The following features are not supported by the Policy Server on Red Hat AS:

- Safeword authentication scheme
- SiteMinder Test Tool

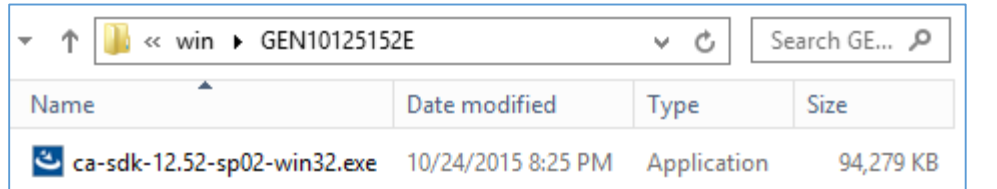
Installation Media and Install Locations

Option 1: SMHOME/bin/smtest.exe

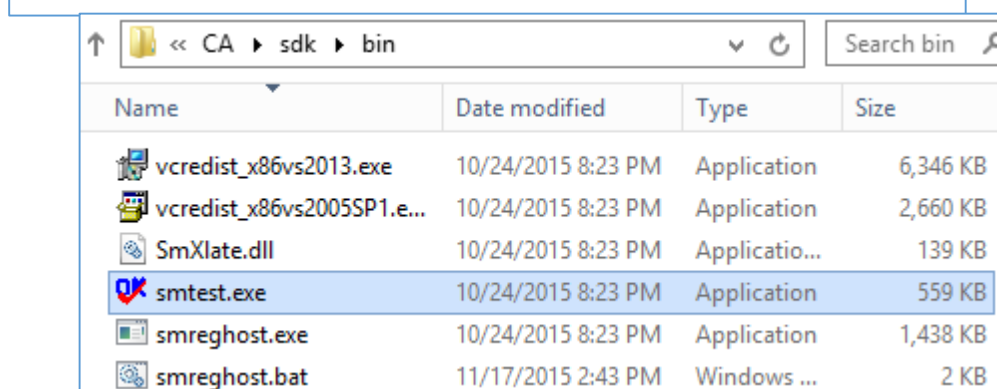
Installed during Win version of SM Policy Server

Option 2: SMSDKHOME/bin/smtest.exe

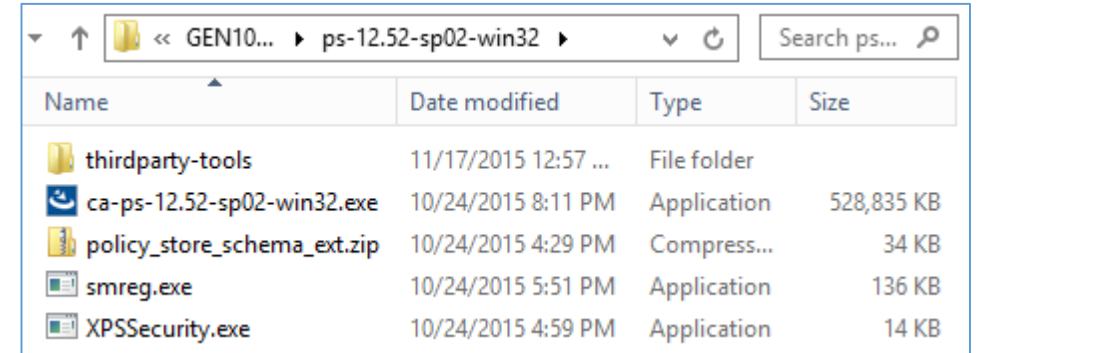
Installed during Win version of SM SDK



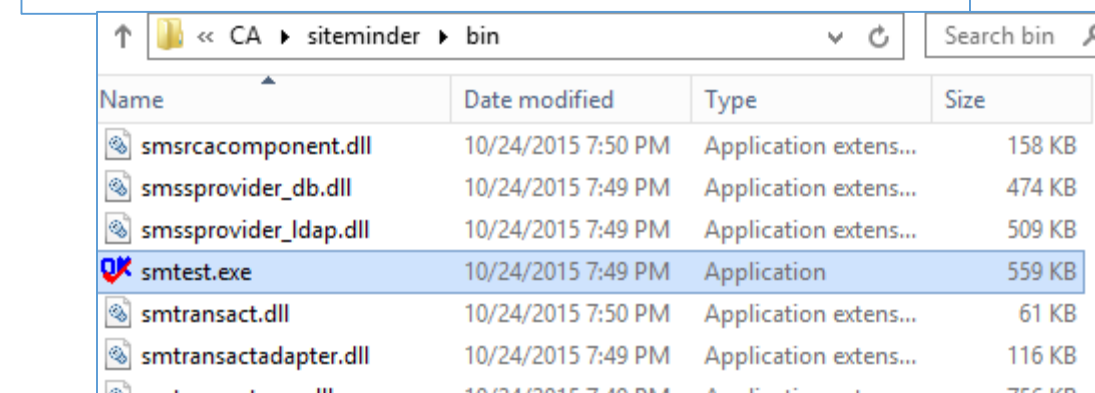
Name	Date modified	Type	Size
ca-sdk-12.52-sp02-win32.exe	10/24/2015 8:25 PM	Application	94,279 KB



Name	Date modified	Type	Size
vcredist_x86vs2013.exe	10/24/2015 8:23 PM	Application	6,346 KB
vcredist_x86vs2005SP1.e...	10/24/2015 8:23 PM	Application	2,660 KB
SmXlate.dll	10/24/2015 8:23 PM	Applicatio...	139 KB
smtest.exe	10/24/2015 8:23 PM	Application	559 KB
smregghost.exe	10/24/2015 8:23 PM	Application	1,438 KB
smregghost.bat	11/17/2015 2:43 PM	Windows ...	2 KB



Name	Date modified	Type	Size
thirdparty-tools	11/17/2015 12:57 ...	File folder	
ca-ps-12.52-sp02-win32.exe	10/24/2015 8:11 PM	Application	528,835 KB
policy_store_schema_ext.zip	10/24/2015 4:29 PM	Compress...	34 KB
smreg.exe	10/24/2015 5:51 PM	Application	136 KB
XPSecurity.exe	10/24/2015 4:59 PM	Application	14 KB



Name	Date modified	Type	Size
smsrcacomponent.dll	10/24/2015 7:50 PM	Application extens...	158 KB
smssprovider_db.dll	10/24/2015 7:49 PM	Application extens...	474 KB
smssprovider_idap.dll	10/24/2015 7:49 PM	Application extens...	509 KB
smtest.exe	10/24/2015 7:49 PM	Application	559 KB
smtransact.dll	10/24/2015 7:50 PM	Application extens...	61 KB
smtransactadapter.dll	10/24/2015 7:49 PM	Application extens...	116 KB

UNIX (Solaris Sparc/x86/AIX) version mentioned but not observed
Linux (RHEL) version NOT available per bookshelf


Policy Server View

Executed from
SMHOME/bin/sctest.exe

CA Single Sign-On Test Tool

Single Sign-On Agent
Agent type: ☒ Version 4 ☐ Version 5 ☐ RADIUS
Agent name:
Secret:
Server:







Policy Server
Policy Server: ☒ Primary ☐ Secondary
IP address:
Authorization port:
Authentication port:
Accounting port:
Request Timeout: secs

Connect to Server
☒ Failover ☐ Round Robin


Mode
☒ Interactive ☐ Record ☐ Basic Playback ☐ Advanced Playback

Resource Information
Resource: Action:
Realm name:
Realm OID:
Credentials:
Redirect:

User Information
Username:
Password:
☐ CHAP Password
Certificate file (b64 DER):

Command







Server Response
Message: Session ID:
Attributes: Reason: Encoding Spec:

Script information
Input Script:
Output Script:

Comment:
Repeat count:
Elapsed:

Dependency Walker - [smtest.exe]

File Edit View Options Profile Window Help

SMTEST.EXE

- SMAGENTAPI.DLL
 - SMERRLOG.DLL
 - ADVAPI32.DLL
 - FAULTREP.DLL
 - MSVCRT.DLL
 - NTDLL.DLL
 - KERNEL32.DLL
 - KERNELBASE.DLL
 - ADVAPI32.DLL
 - RPCRT4.DLL
 - WER.DLL
 - MSVCRT.DLL
 - API-MS-WIN-CORE-HEAP-L1-2-0.DLL
 - API-MS-WIN-CORE-LIBRARYLOA...
 - API-MS-WIN-CORE-REGISTRY-L...
 - API-MS-WIN-CORE-ERRORHAND...
 - API-MS-WIN-CORE-SYSINFO-L1...

Validate dependencies for smtest.exe

E	Ordinal ^	Hint	Function
C++	1 (0x0001)	0 (0x0000)	??0CRegistry@@QAE@ABV0@@@Z
C++	2 (0x0002)	1 (0x0001)	??0CSmAgentTliSocketUtils@@@QAE@XZ
C++	3 (0x0003)	2 (0x0002)	??0CSmAgentTliClientSocketProvider@@@QAE@I@Z
C++	4 (0x0004)	3 (0x0003)	??0CSmAgentTliCryptoProvider@@@QAE@XZ
C++	5 (0x0005)	4 (0x0004)	??0CSmAgentTliHandleSet@@@QAE@ABV0@@@Z
C++	6 (0x0006)	5 (0x0005)	??0CSmAgentTliHandleSet@@@QAE@XZ
C++	7 (0x0007)	6 (0x0006)	??0CSmAgentTliHandleSetIterator@@@QAE@AAVCSmAgentTliHandleSet@@@H@Z
C++	8 (0x0008)	7 (0x0007)	??0CSmAgentTliServerSocketProvider@@@QAE@XZ

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	P
IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).									
WLANAPI.DLL	Error opening file. The system cannot find the file specified (2).									
API-MS-WIN-CORE-SYNCH-L1-1-0.DLL	07/25/2012 8:46p	07/25/2012 8:46p	3,584	HA	0x00004DFE	0x00004DFE				
SHCORE.DLL	09/28/2015 8:02p	09/28/2015 4:13p	452,608	A	0x0007AC4A	0x0007AC4A				
SHLWAPI.DLL	07/25/2012 9:19p	07/25/2012 5:26p	246,784	A	0x0004B969	0x0004B969				
EXT-MS-WIN-ADVAPI32-PSM-APP-L1-1-0.DLL	07/25/2012 8:41p	07/25/2012 8:41p	3,072	HA	0x0000B8BC	0x0000B8BC				
EXT-MS-WIN-NTUSER-MESSAGE-L1-1-0.DLL	07/25/2012 8:40p	07/25/2012 8:40p	3,584	HA	0x0000F796	0x0000F796				
IEFRAME.DLL	10/20/2015 9:00a	10/20/2015 8:51a	13,775,360	A	0x00D2E2EF	0x00D2E2EF				

depends22_x86 Application Tools

File Home Share View Manage

Copy Paste Move to Delete Copy to Rename New folder Properties Select

Clipboard Organize New Open

scripts depends22_x86

Name	Date modified	Type	Size
depends.chm	10/29/2006 2:20 AM	Compiled HTML ...	161 KB
depends.dll	10/29/2006 2:20 AM	Application extens...	9 KB
depends.exe	10/29/2006 2:20 AM	Application	799 KB

3 items 1 item selected 798 KB

Dependency Walker 2.2

CA IAM Connector Server

Dependency Walker is a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys, etc.) and builds a hierarchical tree diagram of all dependent modules. For each module found, it lists all the functions that are exported by that module, and which of those functions are actually being called by other modules. Another view displays the minimum set of required files, along with detailed information about each file including a full path to the file, base address, version numbers, machine type, debug information, and more.

Dependency Walker is also very useful for troubleshooting system errors related to loading and executing modules. Dependency Walker detects many common application problems such as missing modules, invalid modules, import/export mismatches, circular dependency errors, mismatched machine types of modules, and module initialization failures.

Dependency Walker runs on Windows 95, 98, Me, NT, 2000, XP, 2003, Vista, 7, and 8. It can process any 32-bit or 64-bit Windows module, including ones designed for Windows CE. It can be run as graphical application or as a console application. Dependency Walker handles all types of module dependencies, including implicit, explicit (dynamic / runtime), forwarded, delay-loaded, and injected. A detailed help is included.

Dependency Walker is completely free to use. However, you may not profit from the distribution of it, nor may you bundle it with another product.

The “depends” tool was used to identify & validate any “hard” dependencies before creating an copy of the smtest folder on a workstation (independent of the full SDK or SMPS installations)



The program can't start because mfc120u.dll is missing from your computer. Try reinstalling the program to fix this problem.

MFC120U.DLL Properties

General Digital Signatures Security Details Previous Versions



MFC120U.DLL

Type of file: Application extension (.DLL)

Opens with: Unknown application

Change...

Location: C:\windows\system32

Size: 4.24 MB (4,449,952 bytes)

Size on disk: 4.24 MB (4,452,352 bytes)

Created: Saturday, October 5, 2013, 3:38:22 AM

Modified: Saturday, October 5, 2013, 3:38:22 AM

Accessed: Today, November 17, 2015, 1 hour ago

Attributes: ☐ Read-only ☐ Hidden

Advanced...

OK

Cancel

Apply

OK

Goal: Create OFFLINE copy of smtest tool.

1. Copy the sdk bin folder from SDK install folder to workstation

Note that one dependency is missing.

2. Execute the included MS VC++ 2013 x86 libraries.

3. Execute smtest.exe again.

Application Tools

bin

Home Share View Manage

<< installmedia >> ca > sm_r12-52 > win > smtest > bin

Search bin

Name	Date modified	Type	Size
vcredist_x86vs2013.exe	10/24/2015 8:23 PM	Application	6,346 KB
vcredist_x86vs2005SP1.exe	10/24/2015 8:23 PM	Application	2,660 KB
SmXlate.dll	10/24/2015 8:23 PM	Application extens...	139 KB
smtest.exe	10/24/2015 8:23 PM	Application	559 KB
smreghost.e			
smreghost.b			



Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them.

☒ I agree to the license terms and conditions

Install

Close



Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005



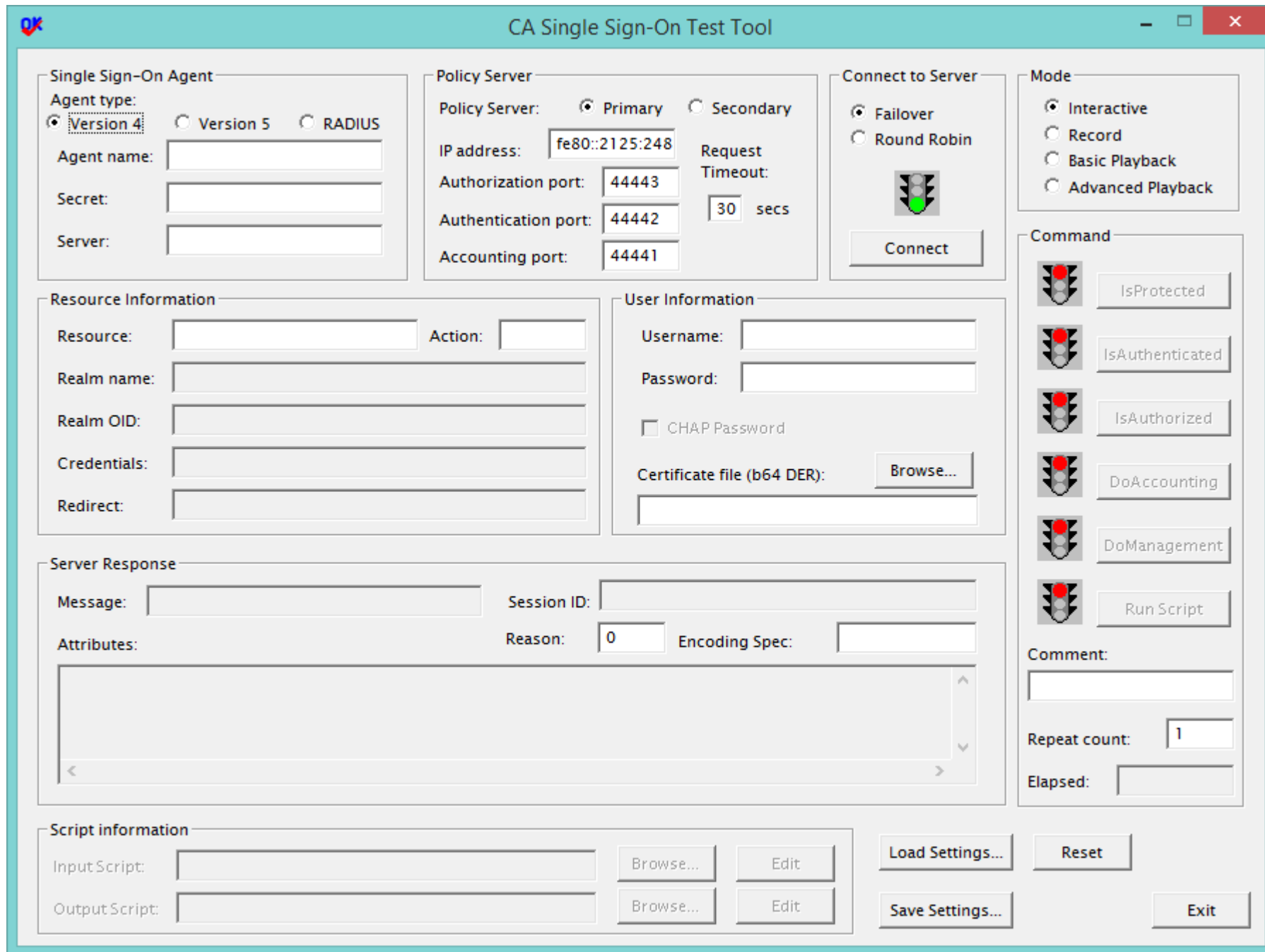
Microsoft Visual C++ 2013
Redistributable (x86) - 12.0.21005

Setup Successful

Workstation View

Executed from Workstation
Folder/bin/sctest.exe

After applying MS VC++ 2013
x86 libraries.




The image shows the 'CA Single Sign-On Test Tool' window. It has a teal title bar with a logo on the left and standard window controls on the right. The interface is divided into several sections: 'Single Sign-On Agent' (Agent type: Version 4, Version 5, or RADIUS; Agent name, Secret, and Server fields), 'Policy Server' (Policy Server: Primary or Secondary; IP address, Authorization port, Authentication port, Accounting port, and Request Timeout), 'Connect to Server' (Failover or Round Robin; a traffic light icon and a Connect button), 'Mode' (Interactive, Record, Basic Playback, or Advanced Playback), 'Resource Information' (Resource, Action, Realm name, Realm OID, Credentials, Redirect), 'User Information' (Username, Password, CHAP Password checkbox, Certificate file (b64 DER) with a Browse... button), 'Server Response' (Message, Session ID, Attributes, Reason, Encoding Spec), 'Script information' (Input Script, Output Script, Browse... and Edit buttons), and a right-hand panel with buttons for IsProtected, IsAuthenticated, IsAuthorized, DoAccounting, DoManagement, Run Script, and a Comment field with Repeat count and Elapsed time. At the bottom right are Load Settings..., Save Settings..., Reset, and Exit buttons.

CA Single Sign-On Test Tool

Single Sign-On Agent
Agent type:
☒ Version 4 ☐ Version 5 ☐ RADIUS
Agent name:
Secret:
Server:

Policy Server
Policy Server: ☒ Primary ☐ Secondary
IP address:
Authorization port:
Authentication port:
Accounting port:
Request Timeout: secs

Connect to Server
☒ Failover ☐ Round Robin

Connect

Mode
☒ Interactive
☐ Record
☐ Basic Playback
☐ Advanced Playback

Resource Information
Resource: Action:
Realm name:
Realm OID:
Credentials:
Redirect:

User Information
Username:
Password:
☐ CHAP Password
Certificate file (b64 DER): Browse...

Server Response
Message: Session ID:
Attributes: Reason: Encoding Spec:

Script information
Input Script: Browse... Edit
Output Script: Browse... Edit

IsProtected
IsAuthenticated
IsAuthorized
DoAccounting
DoManagement
Run Script
Comment:
Repeat count:
Elapsed:

Load Settings... Reset
Save Settings... Exit

OOTB SM POLICY BIN FOLDER

Warning: At least one delay-load dependency module was not found
Warning: At least one module has an unresolved import due to a missing DLL in search path

OOTB SM SDK BIN FOLDER

Warning: At least one delay-load dependency module was not found
Warning: At least one module has an unresolved import due to a missing DLL in search path

NOTE: Tested with the older MS VC++ 2005SP1 libraries but no change.

Note: On X64 OS system, the "soft" dependencies may NOT be in the PATH; these files may be under C:\Windows\System32\downlevel

COPY FROM SDK TO WORKSTATION

Error: At least one required implicit or forwarded dependency was not found
Warning: At least one delay-load dependency module was not found
Warning: At least one module has an unresolved import due to a missing DLL in search path

NOTE: The below dependencies appear to be "soft" and not required for smtext.exe to function.

Dependency Walker - [api-ms-win-core-synch-l1-1-0.dll]

File Edit View Options Profile Window Help

API-MS-WIN-CORE-SYNCH-L1-1-0.DLL

Windows 2012 x64

Location: (in PATH)
C:\Windows\System32

PI	Ordinal ^	Hint	Function	Entry Point
E	Ordinal ^	Hint	Function	Entry Point
1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	0x0000105A	
2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	0x0000105A	
3 (0x0003)	2 (0x0002)	CancelWaitableTimer	0x0000106C	
4 (0x0004)	3 (0x0003)	CreateEventA	0x0000108A	
5 (0x0005)	4 (0x0004)	CreateEventExA	0x0000108A	
6 (0x0006)	5 (0x0005)	CreateEventExW	0x0000108A	
7 (0x0007)	6 (0x0006)	CreateEventW	0x0000108A	

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base
API-MS-WIN-CORE-SYNCH-L1-1-0.DLL	07/25/2012 8:46p	07/25/2012 8:46p	3,584	HA	0x00004DFE	0x00004DFE	x86	Console	CV	0x10000000	Unknown

System and Security > System

View basic information about your computer

Windows edition

Windows Server 2012 Standard

© 2012 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz 2.65 GHz (2 processors)

Installed memory (RAM): 2.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Dependency Walker - [api-ms-win-core-synch-l1-1-0.dll]

File Edit View Options Profile Window Help

API-MS-WIN-CORE-SYNCH-L1-1-0.DLL

Windows 2012 R2 x64

Location: (NOT in PATH)
C:\Windows\System32\downlevel

PI	Ordinal ^	Hint	Function	Entry Point
E	Ordinal ^	Hint	Function	Entry Point
1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	kernel32.AcquireSRWLockE	
2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	kernel32.AcquireSRWLockS	
3 (0x0003)	2 (0x0002)	CancelWaitableTimer	kernel32.CancelWaitableTi	
4 (0x0004)	3 (0x0003)	CreateEventA	kernel32.CreateEventA	
5 (0x0005)	4 (0x0004)	CreateEventExA	kernel32.CreateEventExA	
6 (0x0006)	5 (0x0005)	CreateEventExW	kernel32.CreateEventExW	
7 (0x0007)	6 (0x0006)	CreateEventW	kernel32.CreateEventW	

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base
API-MS-WIN-CORE-SYNCH-L1-1-0.DLL	08/22/2013 7:25a	08/21/2013 10:17p	4,608	A	0x00010DD9	0x00010DD9	x86	Console	CV	0x10000000	Unknown

System and Security > System

View basic information about your computer

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

System

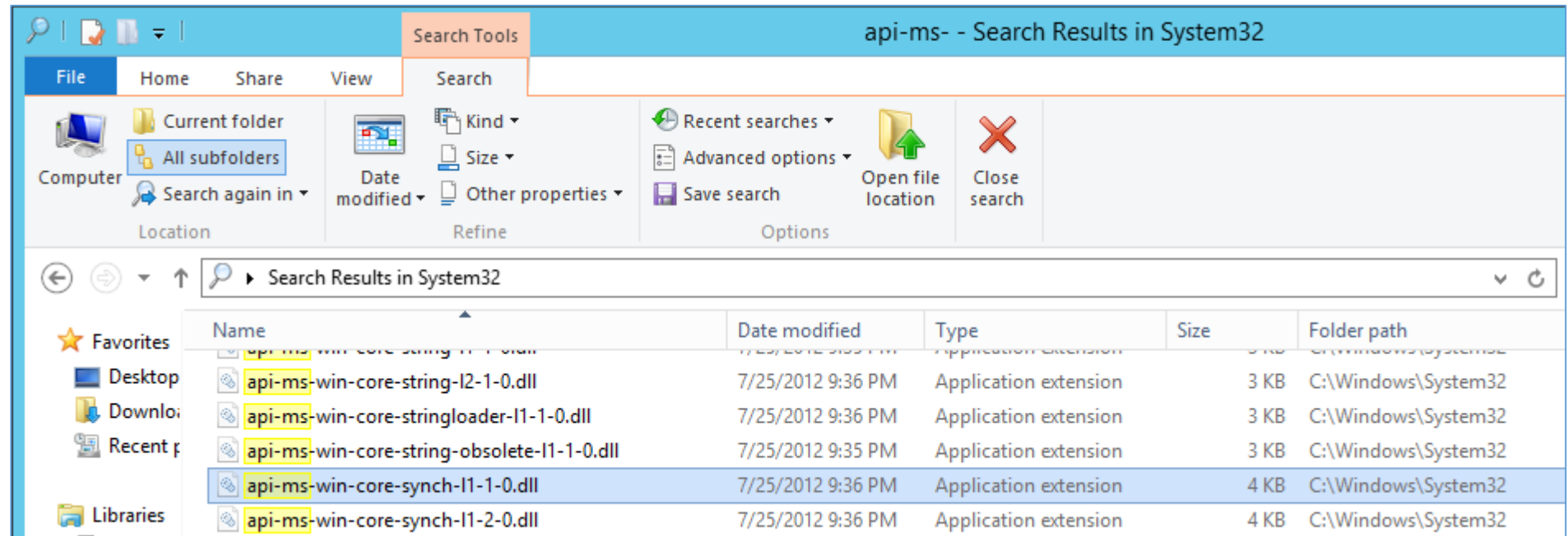
Processor: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz 2.66 GHz

Installed memory (RAM): 24.0 GB

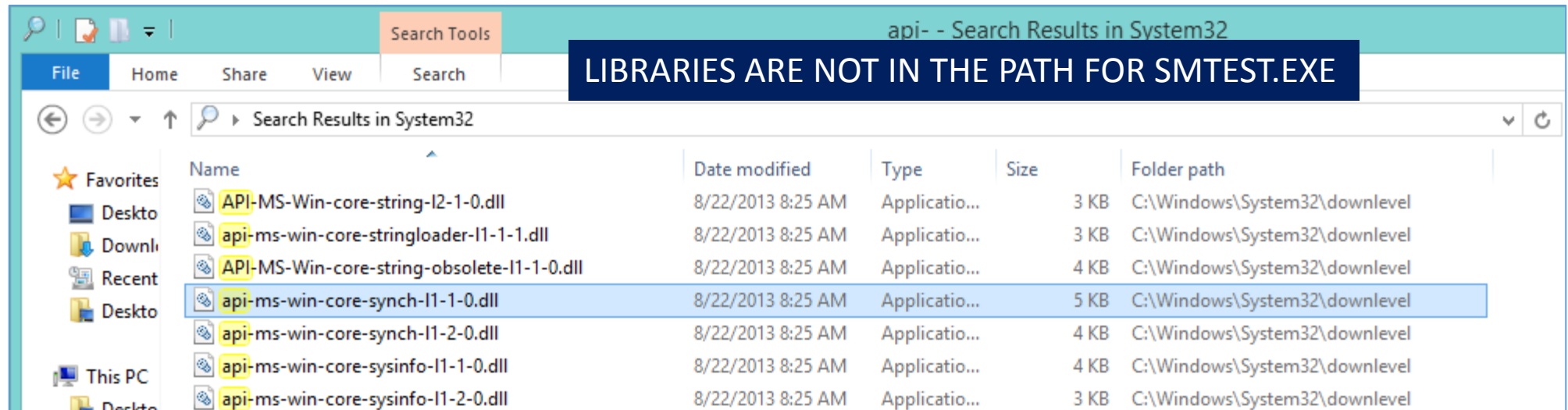
System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

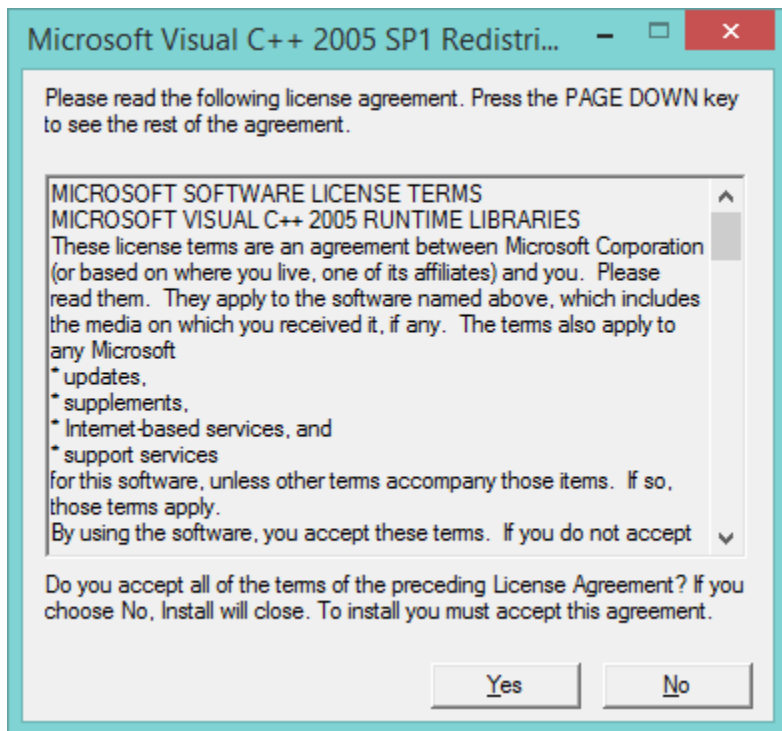
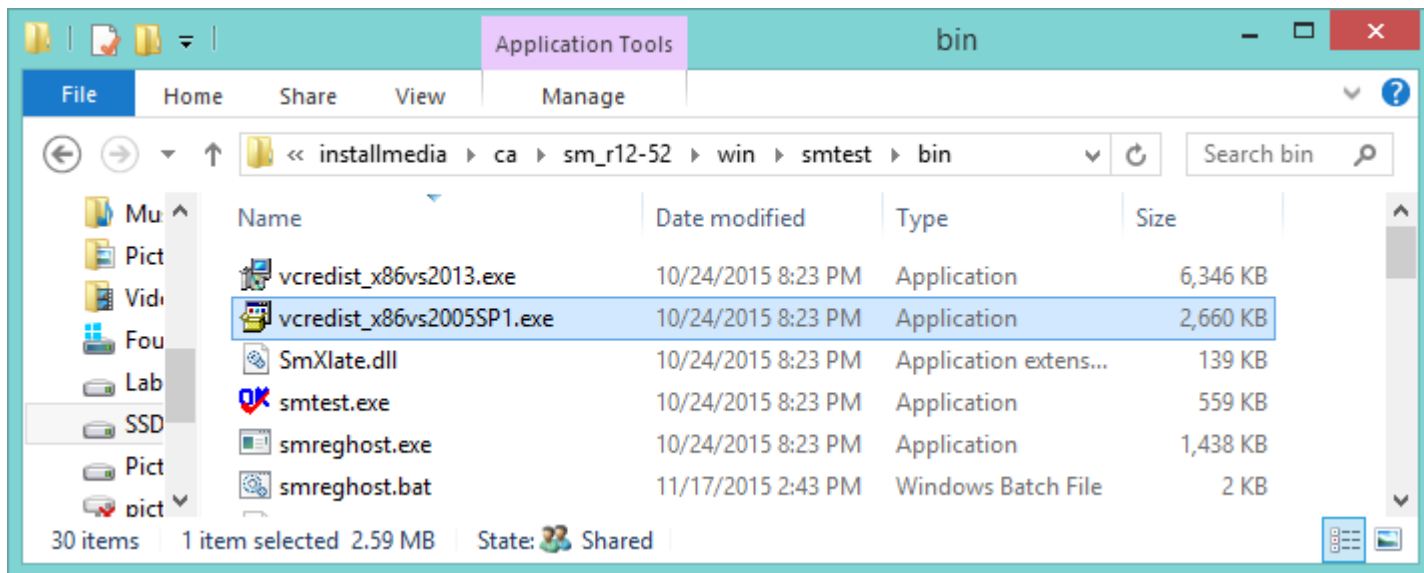
Windows 2012 x64



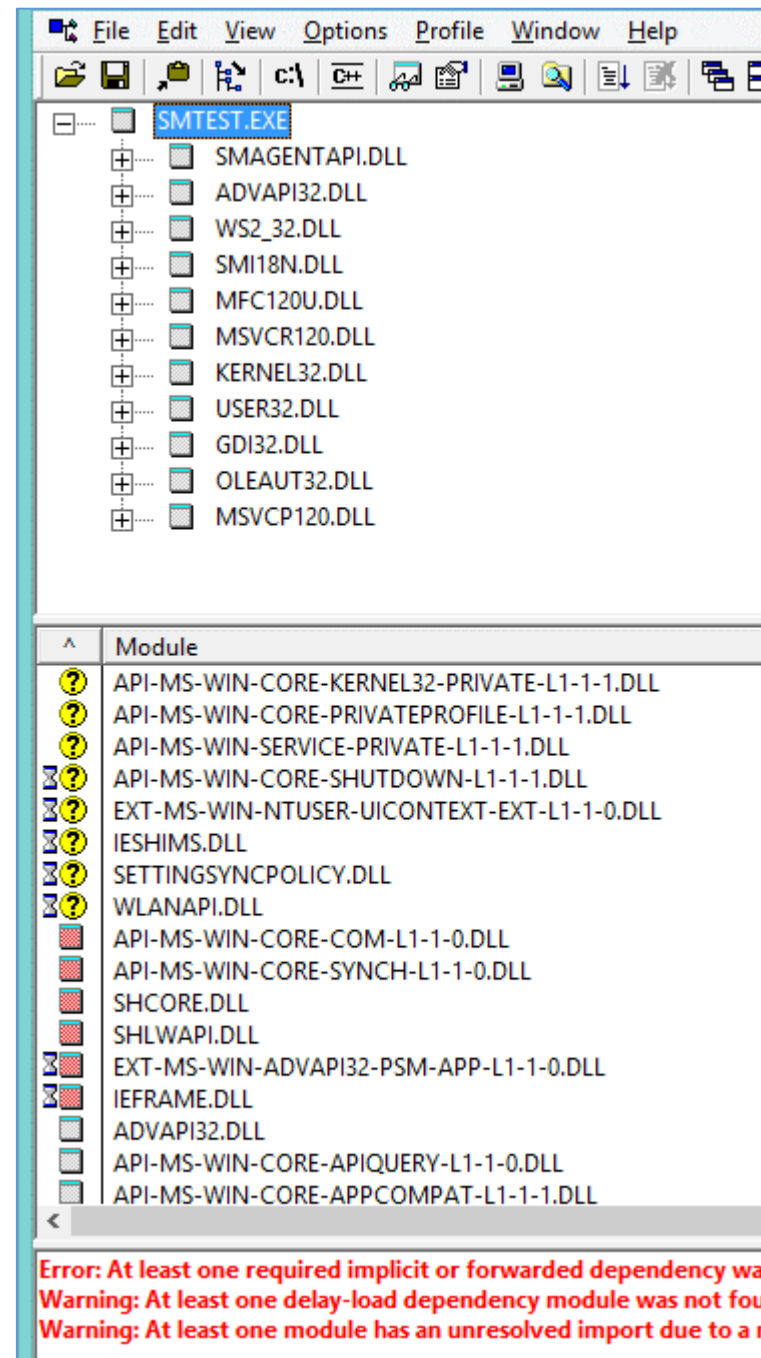
Windows 2012 R2 x64



If there is an issue, then C:\Windows\System32\downlevel may be added to the PATH environmental variable



Observation:
No change or impact
with use of the MS VC++
2005 SP1 libraries
deployed, based on
results from Dependency
Walker tool

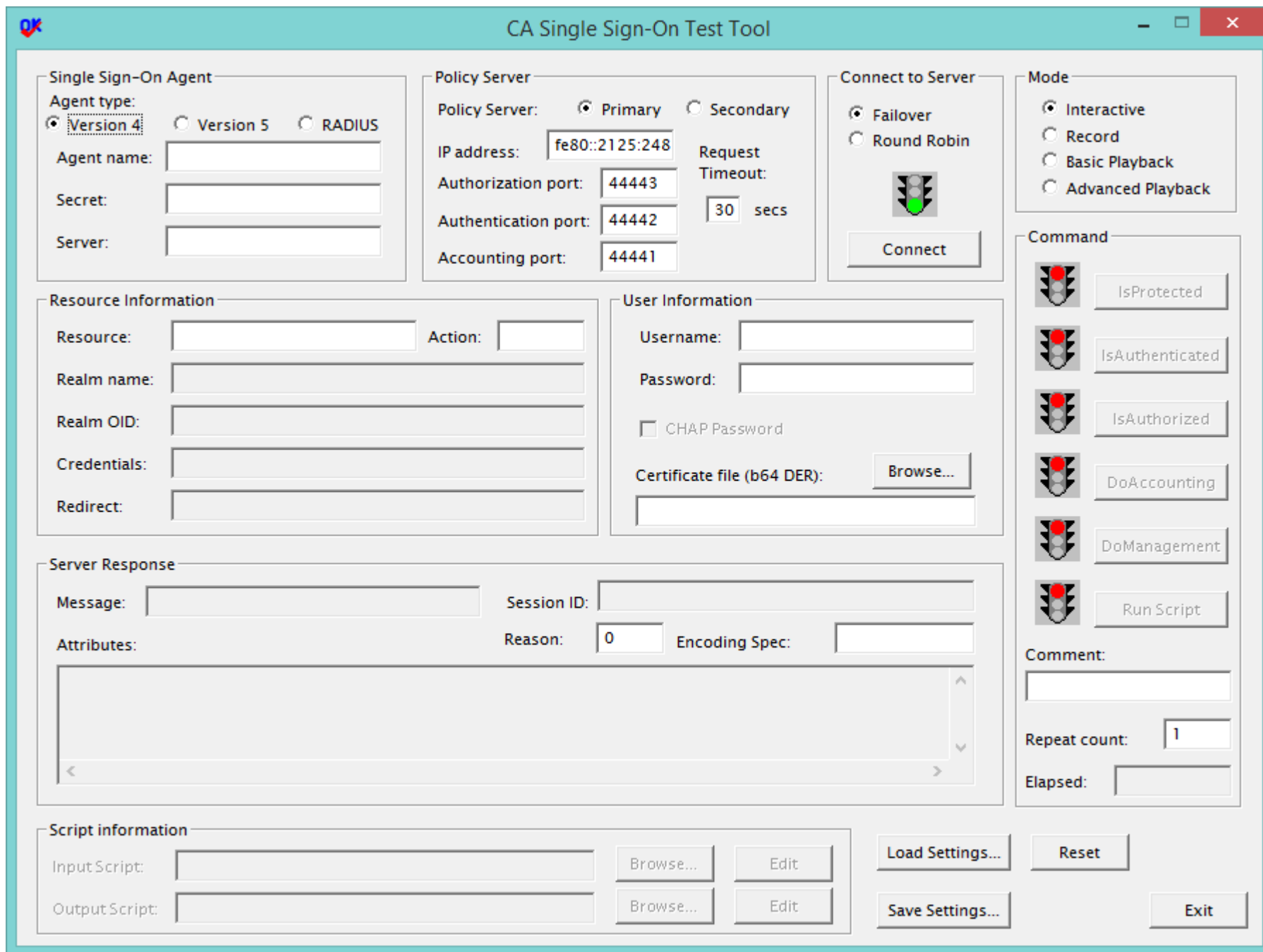


Workstation View

Executed from Workstation
Folder/bin/**smtest.exe**

Note: Pre-work Steps to use for 5.x Agents
(Not required for 4.x agents)

1. Copy the SmHost.conf from an existing Web Agent Deployment or create one.
2. Open a command line window to the bin folder. Then execute the **smreghost.exe** to make your workstation/laptop a trusted host to the SM Policy Server.
 - a. (Not required for 4.x agents)



The image shows the 'CA Single Sign-On Test Tool' window. It is divided into several sections for configuring and testing single sign-on agents.

- Single Sign-On Agent:** Includes fields for Agent type (Version 4 selected), Agent name, Secret, and Server.
- Policy Server:** Includes fields for Policy Server (Primary selected), IP address (fe80::2125:248), Authorization port (44443), Authentication port (44442), Accounting port (44441), and Request Timeout (30 secs).
- Connect to Server:** Includes radio buttons for Failover (selected) and Round Robin, a traffic light icon, and a Connect button.
- Mode:** Includes radio buttons for Interactive (selected), Record, Basic Playback, and Advanced Playback.
- Resource Information:** Includes fields for Resource, Action, Realm name, Realm OID, Credentials, and Redirect.
- User Information:** Includes fields for Username, Password, a checkbox for CHAP Password, Certificate file (b64 DER) with a Browse... button, and a text field.
- Server Response:** Includes fields for Message, Session ID, Attributes, Reason (0), and Encoding Spec, with a large text area for the response.
- Script information:** Includes fields for Input Script and Output Script, each with a Browse... button and an Edit button.
- Command:** Includes a vertical list of buttons: IsProtected, IsAuthenticated, IsAuthorized, DoAccounting, DoManagement, and Run Script, each with a traffic light icon.
- Comment:** Includes a text field and a Repeat count field (1).
- Elapsed:** Includes a text field.
- Buttons:** Load Settings..., Save Settings..., Reset, and Exit.

Copy of smtest.exe from CA SSO SDK r12.52



smtest_r12-52_windows.zip

Additional Information Pulled from SSO Bookshelf / Tech Notes & Reformatted

Run smtest from command line

<Siteminder_root_path>\bin>**smtest controlfile.txt /c**

Here are the list of smtest options:

SmTest --> opens the SmTest Windows UI without initial settings

SmTest <Init_file> --> opens the SmTest Windows UI with initial settings

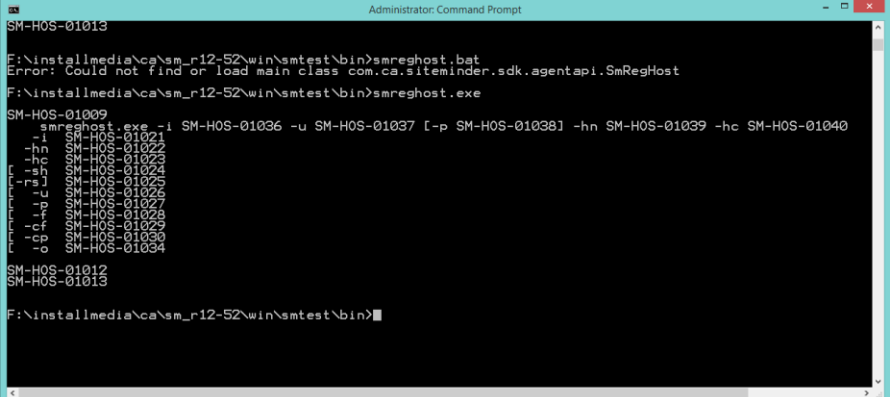
SmTest <Input_file> <Output_file> --> runs Basic Playback mode without opening the Windows UI

SmTest <Input_file> /F --> runs Basic Playback mode with default output file at DOS

SmTest <Control_file> /C --> runs Advanced Playback mode without opening the Windows

After the test finishes, there is a stats file generated under the same directory of the input.txt file with the file name as <the input filename>_stats, e.g input.txt_stats. It contains some useful information of the test.

Run the smreghost from the Windows command prompt to make your laptop a trusted host and you are good to go.



```
Administrator: Command Prompt
SM-H0S-01013
F:\installmedia\ca\sm_r12-52\win\smtest\bin\smreghost.bat
Error: Could not find or load main class com.ca.siteminder.sdk.agentapi.SmRegHost
F:\installmedia\ca\sm_r12-52\win\smtest\bin\smreghost.exe
SM-H0S-01009
smreghost.exe -l SM-H0S-01036 -u SM-H0S-01037 [-p SM-H0S-01038] -hn SM-H0S-01039 -hc SM-H0S-01040
SM-H0S-01012
SM-H0S-01013
F:\installmedia\ca\sm_r12-52\win\smtest\bin>
```

Ref: **How to run smtest on command line?**

<http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec547520.aspx>

SMTEST Control File: controlfile.txt

Requires three (3) files under the SmTestTool folder.

1. Control File. (e.g. see below / controlfile.txt / Input file)
2. Recorded File (e.g. smtestrecord.txt / output file)
3. Settings File (ini, created from 1st run of SMTEST & saved as ini file; Do NOT create or manually edit this file; allow smtest.exe to create.)

controlfile.txt

```
.verbose
.sleep 5000
.connect smtest.ini
C:\temp\smtest\smtestrecord.txt, 50, 10
.disconnect
.report
.output
.viewstats
```

Note: To force CSV format for output / playback file
setx /m SMTESTCSVFILE "pathname of the CSV file"

Command	Description
.report	Generates a final report (as an output file) summarizing the test results. The report does not include the status of each server request. This is the default.
.reportsread	Generates a file containing a response time spread report. The file name is <i>command_script_stats_spread</i> (for example, isprotected-record.txt_stats_spread).
.output	Generates a final report (as an output file) summarizing the overall results including the status of each server request.
.viewstats	Displays final statistics in a text editor.
.verbose	Generates output files containing the details of each server request.
.brief	Generates output files containing the brief results of each server request. This option is only valid when used with the .output command.
.sleep	Lets the Test Tool pause for a specified amount of time (in milliseconds). This simulates intermittent server requests.
.userselectionmode	Determines whether usernames are used sequentially or selected randomly. Valid values are 0 (sequential) and 1 (random). For more information, see (Optional) Configure How the Test Handles Usernames .
.randomseed	Allows the pseudo-random sequence of names to be repeated (up to thread ordering) for each test. For more information, see (Optional) Configure How the Test Handles Usernames .
.connect settings_file	Initializes the Test Tool using information from the Test Tool Settings file to set up a multi-threaded test with one simulated Agent. The default multi-threaded test comprises multiple simulated Agents with one simulated Agent per thread. You can also set up a test with one simulated Agent and multiple threads by using this option.
.disconnect	Un-initializes the Test Tool to indicate the end of one simulated Agent multi-threaded test.

SiteMinder Test Tool: SSO Bookshelf Links

This section contains the following topics:

[Test Tool Overview](#)

[Configure Your Test Environment Agent](#)

[Run a Functionality Test](#)

[Perform a Regression Test by Playing Back a Test Recorded in a Command Script File](#)

[Run a Stress Test](#)

[Certificate-based Authentication Tests](#)

SiteMinder Test Tool: Overview

Test Tool Overview

- ❑ The CA SiteMinder® Test Tool is a utility that simulates the interaction between Agents and Policy Servers. It tests the functionality of the Policy Server. During testing, the Test Tool acts as the Agent, making the same requests to the Policy Server as a real Agent. This allows you to test your CA SiteMinder® configuration before deploying it.
- ❑ The CA SiteMinder® Test Tool is only available on Windows systems. It can be used to emulate Windows-based Web Agents and RADIUS Agents without limitations. The CA SiteMinder® Test Tool can create connections with any Policy Server on all platforms, however, post 4.x Web Agents on Solaris cannot be tested with the CA SiteMinder® Test Tool.
- ❑ To test policies for CA SiteMinder® 5.x and later Web Agents, do one of the following:
 - Use the Perl scripting interface for Web Agent registration and testing.
 - Install and configure the CA SiteMinder® Web Agent and test it manually.

The CA SiteMinder® Test Tool performs three types of tests:

- ❑ Functionality - Tests policies to ensure they are configured correctly.
- ❑ Regression - Tests whether or not changes, such as migrating a policy store or implementing a new feature, affect CA SiteMinder®.
- ❑ Stress - Tests the performance of the Policy Server as it receives multiple requests.

Note: You can also test policies using the Scripting Interface. See the Programming Guide for Perl.

SiteMinder Test Tool – Configure SM Agent

Configure Your Test Environment Agent

You can configure the Agent that the Test Tool simulates during a test in the CA SiteMinder® Agent group box.

The Agent that the Test Tool simulates must be configured in the Administrative UI.

To configure Agent information, specify the following options

Agent Type Specify one of the following Agent Types:

- | | |
|-----------|--------------------------------------|
| Version 4 | Simulates CA SiteMinder® 4.x Agents. |
| Version 5 | Simulates CA SiteMinder® 5.x Agents. |

Note: If you want to use the Test Tool on a system to simulate a CA SiteMinder® 5.x Web Agent, you must run the **smreghost.exe** application on the system where you will run the Test Tool. The smreghost.exe file is included with your Web Agent, and described in the Web Agent Installation Guide. The file is also located in <Policy Server install dir>/siteminder/bin.

RADIUS	Simulates RADIUS devices.
--------	---------------------------

Agent Name Enter the name of the Agent as it appears in the Administrative UI. This field is required for both Version 4 and Version 5 Agent simulations.

Secret Enter the Agent's shared secret. This must match the shared secret entered when the Agent was created. A Secret is required for Version 4 and RADIUS Agent simulations.

(Optional) Server Enter the full name of the server on which the Agent resides. For example, to test the Policy Server for <http://www.myorg.org>, enter www.myorg.org in this field. This field may be used for Version 4 Agent simulations.

SmHost.conf Path Enter the path to the SmHost.conf file that contains the settings for the Version 5 Agent you want to simulate. You can use the Browse button to search for the SmHost.conf file.

Start the Test Tool on Windows to test Policy Server functionality.

Important! If you are accessing the Test Tool on Windows Server 2008, open the shortcut with Administrator permissions. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

In a Command Window, navigate to policy_server_home\bin and enter the following command:
smtest.exe

Start the Test Tool on UNIX to test Policy Server functionality.

Open a Command Window and navigate to policy_server_home/bin.
Type the following command:

./smtest NOT available for RHEL Linux per Bookshelf Notes

Note: To run the Test Tool on UNIX, the X display server must be running. If required, enable the display by entering the following in a Command Window:

export DISPLAY=n.n.n.n:0.0 Where n.n.n.n, specifies the IP address of the Policy Server host system.

How to Use the Test Tool in FIPS-only Environments (See bookshelf)

COMPAT (Default) Encrypt sensitive data using a non-FIPS algorithm when recording a Command Script file. Decrypt sensitive data that is written to a Command Script file using non-FIPS or FIPS algorithms when playing back a test.

SiteMinder Test Tool – Policy Server & SmHost.conf

Policy Server Identification

The test tool requires information about the Policy Server that will be used when simulating the interaction with the Agent described in the CA SiteMinder® Agent group box. The required information differs slightly depending on the type of Agent you selected.

To set up Policy Server(s) for **Version 4 Agent** and RADIUS Agent simulations

Specify the following Policy Server options, as necessary:

Policy Server Indicates whether you are specifying the primary or secondary Policy Server.

IP Address Specifies the IP address of the Policy Server. By default, this field contains the IP address of the local system.

Authorization, Authentication, and Accounting Ports Specifies the TCP ports used for authorization, authentication, and accounting requests. These fields are populated with the Policy Server's default port numbers.

Timeout Displays the time (in seconds) that the Test Tool should wait for a response from the Policy Server.

Select one of the following operation modes:

Failover Enables failover. During failover, the Test Tool directs requests to the initial Policy Server. If the initial Policy Server fails, the Test Tool redirects requests to the secondary Policy Server.

Round Robin Enables round robin load balancing. Round robin load balancing divides requests between the primary and secondary Policy Servers. For each connection, the Test Tool alternates between Policy Servers.

Click Connect to make sure that the Test Tool can connect to the Policy Server. If the Test Tool makes a connection, the IsProtected and DoManagement stop lights turn green.

Note: You must specify an Agent before testing the Policy Server connection.

Policy Server Information for Version 5 Agents

For Version 5 Agents simulations, you may specify the IP address and port information of the Policy Server(s) used in the test, or you may use the Policy Server information contained in the Host Configuration Object contained in the policy store.

By default, the Policy Server information will be retrieved from the policy store when **the Test Tool uses the SmHost.conf file to establish an initial connection to the Policy Server**. To specify Policy Server information manually, select the Override check box and fill in Policy Server information as described in Set Up the Policy Server for Version 4 Agents and RADIUS Agent Simulations.

Select a Test Mode

Use one of the test modes in the following list to determine how tests are run and results are displayed. Depending on the test mode that you select, you may also have to specify script information.

Interactive Allows you to enter data, run tests, and see the results displayed immediately in the Server Response section.

Record Combines Interactive operation with a script generation feature that writes test results to a plain-text command script file.

Basic Playback Uses Command Script files created in the Record mode to automate sequential tests. Ideal for regression testing.

Advanced Playback Uses a manually configured Thread Control File to automate complex tests. Ideal for stress testing.

Run a Stress Test

You can specify the resource against which you want to conduct tests. Providing a resource simulates a user entering a URL in a browser.

Resource Enter the relative path of the resource that CA SiteMinder® is protecting as it is configured in the realm. The path is relative to the Web server's publishing directory. For example, /protected/.

Action Enter the Agent action, Authentication event, or Authorization event specified in the rule that you are testing.

You can configure the Agent that the Test Tool simulates during a test in the CA SiteMinder® Agent group box.

Specify User Credentials The Test Tool requires user credentials to test whether or not a policy can authenticate or authorize a user.

User Name Enter the user name you want to use to access the resource.

Password Enter the password for the user entered in User Name.

CHAP Password If you are using a RADIUS CHAP authentication scheme, select this check box.

Certificate File If the protected resource requires certificates to authenticate users, you must provide a certificate file so that the Test Tool can simulate certificate authentication.

SiteMinder Test Tool – Encoding & Parameters

Set the Encoding Spec

The encoding spec field allows you to specify a language encoding parameter. The Test Tool uses this parameter to encode headers in the same manner as a Web Agent. It then displays the encoded response attribute data in the Attributes field.

For more information about language encoding, see the Web Agent Configuration Guide.

To set the encoding spec, enter a value for the encoding spec as follows:

encoding_spec, wrapping_spec where:

encoding_spec is a text string that represents one of the following encoding types: UTF-8, Shift-JIS, EUC-J, or ISO-2022 JP

wrapping_spec is the wrapping specification, which must be RFC-2047.

Note: If you leave this field blank, the default is UTF-8 with no wrapping.

You can configure the Agent that the Test Tool simulates during a test in the CA SiteMinder® Agent group box.

Save and Load Test Configurations in a Test Tool Settings File

To avoid reentering user-supplied information, such as Agent, resource, and user information, you can save these values into a Test Tool Settings file. You can then reload those values at any time.

To save the current values that are specified in the Test Tool:

Click the Save Settings button.

Enter a location and name for the Test Tool Settings in the Save As dialog and click Save.

The file is saved with a .ini file extension.

To retrieve the saved values from the Test Tool Settings file:

Click the Load Settings button.

Enter the location and name of the Test Tool Settings File in the Open dialog and click Open.

Note: You can also load the Test Tool Settings file from a Command Script.
(Optional) Regulate Test Tool Connections to the Policy Server

Edit the Test Tool Settings (.ini) file and add the following parameters to regulate how the Test Tool connects to the Policy Server:

MaxConnections = 50 (20 default) Specifies the maximum number of connections that the Test Tool establishes to the Policy Server.

MinConnections = 1 Specifies the minimum number of connections that the Test Tool establishes to the Policy Server.

ConnectionsStep = 5 (2 default) Specifies how many new sockets the Test Tool can be opened at a time if a new connection needs to be made (up to the value specified in MaxConnections:).

Follow these steps:

Check the value of the "SM Agent or Radius:" parameter in the Command Script file and do one of the following steps:

If the "SM Agent or Radius" value is set to SM Agent v4, proceed to Step 3.

If the "SM Agent or Radius" value is set to SM Agent v5, add an "Override Bootstrap:" parameter with a value of 1 to the Command Script file.

Verify that the value of the "Agent Name" parameter in the Command Script file is the same as the "Agent name" parameter in the Test Tool Settings file. If not, the new parameters are ignored and the following default values used: MaxConnections=20, ConnectionStep=2.

Open the Test Tool Settings file in a text editor.

Add required parameters, one per line, using the same format as the other parameters in the file. That is, enter the parameter value starting at column 24 of the line.

Save and close the Test Tool Settings file.

SiteMinder Test Tool: Functionality Test (non-FIPS)

Run a Functionality Test

The CA SiteMinder® Test Tool allows you to test the functionality of policies in a simulated real-world environment. To perform a functionality test, you must have the following:

- A Policy Server that is configured and running
- A CA SiteMinder® Agent that is configured in the Administrative UI

Note: If the Test Tool is simulating a CA SiteMinder® Agent v5.x, that Agent must have 4.x support enabled.
A policy domain configured with any type of user directory AND A policy that pairs a rule with a user(s)

CA SiteMinder® allows you to perform the following functionality tests:

IsProtected Indicates whether or not a policy is protecting the resource you specified.

IsAuthenticated Indicates whether or not the Policy Server can authenticate a set of user credentials against a user directory.

When user credentials are authenticated, the Policy Server compares the credentials to entries in a user directory. If the credentials match an entry, the Policy Server creates a session ticket and authenticates the user.

In a "real" CA SiteMinder® deployment, CA SiteMinder® confirms that a user's session ticket is valid instead of rechecking the user's credentials against a directory when an authenticated user makes additional requests. By default, the Test Tool authenticates the user each time the IsAuthenticated test is run, regardless of whether or not the user has a session ticket.

You can configure the Test Tool to validate a user's session ticket by entering Validate in the Comment field in the Test Tool before running an IsAuthenticated test; however, CA SiteMinder® must authenticate the user before validating the session ticket.

Note: You can specify Validate when you run multiple tests in Interactive mode (using the Repeat count field), and in Playback mode.

IsAuthorized Indicates whether or not the Policy Server can authorize a user based on a policy.

These tests must be run in the order they appear above.

For example, you **must run IsProtected before running IsAuthenticated**.

The order reflects the steps that CA SiteMinder® uses to determine a user's access rights.

While running functionality tests, you can also use the Test Tool to perform the following tasks:

DoAccounting Logs the most recent accounting server transactions.

DoManagement Requests Agent commands, such as cache flush commands that clear the Agent cache. Running DoManagement ensures that the Test Tool receives current information from the Policy Server.

To run a functionality test Configure a test environment.

Note: You can also test policies using the Scripting Interface. See the Programming Guide for Perl.
(Optional) Specify the number of times you want the Test Tool to run your test in the Repeat Count field in the Command group box.

In the Command group box, select one of the following tests to run:

- IsProtected
- IsAuthenticated
- IsAuthorized

If you are running an IsAuthenticated test and you want the Test Tool to validate an authenticated user's session ticket instead of authenticating the user's credentials against a user directory, enter Validate in the Comment field.

Note: Before validating a user's session ticket, the user must be authenticated. Once the user is authenticated, CA SiteMinder® creates a session ticket for the user.

SiteMinder Test Tool: Average Elapsed Time

Calculate an Average Elapsed Time

Configure Your Test Environment Agent

(Optional) Record Your Test in a Command Script File for Regression and Stress Testing

When you run a test in Record mode, the Test Tool writes the test commands and test results to a plain-text Command Script file. This file can later be used as an input file to repeat the test in playback mode.

You can record multiple tests to the same Command Script file. The Test Tool appends the test results to the end of the file. You can then use the script file for regression testing.

Follow these steps:

- Select the Record test mode.

- Enter the path and filename for the Command Script file where the test results are stored in the Output Script field.

- Optionally, enter how many times the recorded test is to run in the Repeat count field.

- Optionally, enter a comment to add to the Command Script file in the Comment field.

- Run one or more tests.

- To stop recording, specify a new test mode.

SiteMinder Test Tool: FIPS Only Functionality Test

How to Use the Test Tool in FIPS-only Environments / Functionality Test Results

The tables in this section describe the results of each type of functionality test.

If isProtected... Then... Succeeds The Test Tool displays Protected in the Message field. This means that the Test Tool made a successful connection to the Policy Server and a policy is protecting the resource.

The Test Tool also populates the following fields with values returned by the Policy Server:

Realm Name Name of the realm that contains the resource
Realm OID The realm object identifier
Credentials The authentication scheme used to protect the resource
Redirect The redirect string used by the authentication scheme, if one is specified. All certificate and HTML forms-based schemes return this string, which typically instructs the Agent where to display a form.

Fails = The Test Tool displays Error or Not Protected in the Message field. Error indicates that the Test Tool could not connect to the Policy Server; Not Protected indicates that the specified resource is not protected by a policy.

If the test fails:
Make sure that the policy is configured correctly.
Check the Authentication server log for debugging information.

If isAuthenticated... Then... Succeeds The Test Tool displays Authenticated in the Message field and populates the following fields with values returned by the Policy Server:

Session ID A unique CA SiteMinder®-assigned session ID. The Policy Server uses this ID to identify the cookie where session information is stored.

Attributes The attributes the Policy Server sends back in the response. For example:
The response indicates the name of the user directory where the user was authenticated.
Note: Click Reset to clear responses displayed in the Attributes field without removing user-supplied information.

Reason The reason code associated with the outcome of the test. This field is used to supply information to developers using the CA SiteMinder® SDK. Reason codes are listed in SmApi.h.

Fails = The Test Tool displays Not Authenticated in the Message field.

If the test fails:
Make sure that you are using valid user credentials.
Check the Authentication server log for debugging information.

If IsAuthorized... Then... Succeeds The Test Tool displays Authorized in the Message field and the CA SiteMinder®-assigned Session ID in the Session ID field. This ID identifies the cookie where session information is stored.

Fails = The Test Tool displays Not Authorized in the Message field.

If the test fails:
Make sure that the policy is configured correctly.
Check the Authorization server log for debugging information.

Calculate an Average Elapsed Time

After performing a test, the Test Tool displays the amount of time the test took to run in the Elapsed Time field of the Command group box. Because of fluctuations in the system, averaging the elapsed time of multiple tests provides more accurate results.

To get an average elapsed time

In the Repeat Count field, specify the number of times you want to run the test.

The Test Tool runs the test the specified number of times and then displays the total elapsed time.
Divide the elapsed time by the number of times the test was run to determine the average elapsed time.

SiteMinder Test Tool: Regression Test

Perform a Regression Test by Playing Back a Test Recorded in a Command Script File

Regression tests allow you to test whether or not changes made to CA SiteMinder®, such as upgrading the policy store or implementing a new feature, affect policies.

To run a regression test, you run one test with the current environment, make changes, then run the test again.

By comparing the results of the tests, you can determine if the changes affect CA SiteMinder®.

To perform a regression test

[Run one or more functionality tests in Record mode.](#)

- Select Basic Playback in the Mode group box.
- Enter the name of the Command Script file in the Input Script field. This file name should match the value you entered in the the Output Script field in Record mode.
- In the Output Script field, specify an output file name.
- In the Command group box, click Run Script. The Test Tool runs the Command Script file and creates the output script file.

SiteMinder Test Tool: Stress Test

Run a Stress Test

The Test Tool allows you to test CA SiteMinder®'s performance when the Policy Server receives more than one request at a time. Using stress tests, you can simulate multiple agents talking to the Policy Server simultaneously or a single agent communicating with the Policy Server on multiple threads.

Stress tests are run in Advanced Playback mode. The Test Tool receives instructions from a Thread Control file that specifies which tests to run and how many times to run them. After executing the instructions in the thread control file, the results of the test are written to an output file.

Configure a Thread Control File

Configure a Thread Control file to define the Command Script files to run, number of repetitions, threads, and so on to automate complex tests for stress testing. A Thread Control file contains multiple instruction lines in the Test Tool's own scripting language and comments, indicated by the # symbol at the beginning of a line.

The basic instructions are in the following format:

command_script_file_name, *repetition_count*, *thread_count*, [*max_time_in_seconds*]

command_script_file_name Specifies the pathname of the previously recorded command script file.

repetition_count Specifies the number of times that the Test Tool runs the Command Script.

thread_count Specifies how many simultaneous threads the Test Tool initiates to run the Command Script.

max_time_in_seconds (Optional) Specifies a limit (in seconds) for the duration of the test. If elapsed test time exceeds this limit then playback halts, regardless of whether the configured number of repetitions are complete.

For example: # c:\temp\test_data.txt, 8, 6, 120

This line specifies that:

- The input Command Script is c:\temp\test_data.txt
- The Test Tool runs the script eight times
- Six simultaneous threads run the script
- The test ends after 120 seconds, regardless of whether eight repetitions are complete

The Test Tool writes the output of the test to a file. The output file name is the name of the input file with _out# appended to it, where # is the incremented thread number. For example, the output files for the test above are c:\temp\test_data.txt_out1 to c:\temp\test_data.txt_out6.

The Test Tool scripting language includes the commands in the following table to control the script file output. See the following figure for a sample thread control file.

Example Thread Control File

```
.output .connect c:\test\smtest.ini .brief c:\temp\test_data1.txt, 2, 3 .verbose .sleep 5000
c:\temp\test_data1.txt, 2, 2 .brief c:\temp\test_data1.txt, 3, 4 .connect smtest.ini c:\temp\test_data1.txt, 5, 6
.disconnect
```

Perform a Stress Test by Running a Thread Control File in Advanced Playback Mode

Use the Advanced Playback test mode to run a stress test defined in a Thread Control file.

Follow these steps:

- 1.Select Advanced Playback in the Mode group box.
- 2.Enter the name of the Thread Control file in the Control field.
- 3.In the Command group box, click Run Script.

The Test Tool runs the Thread Control file and creates an output script file.

SiteMinder Test Tool: Stress Test Options

(Optional) Configure How the Test Handles Usernames

The following three parameters configure how a test handles usernames.

34 UserCount:

(Defined in the Command Script file.) Specifies the number of users of the format AAAAAA, BAAAAA, through ZZZZZZ that the test uses for authentication and authorization. If the UserCount: parameter is set, the Username: parameter is ignored.

Note: Although it is ignored, the Username: parameter is still required. Do not delete it. Add the UserCount: parameter using the same format as the other parameters in the Command Script file. That is, enter the complete parameter name (including the "34 " prefix) and the parameter value starting at column 24 of the line.

For example: **34 UserCount: 1000**

.userselectionmode

(Defined in the Thread Control File) Determines whether usernames are selected sequentially or randomly. Valid values are 1 and 2.

If set to **1**, the test steps sequentially step through usernames until the value specified by the UserCount parameter is reached. Usernames then wrap back to "AAAAAA" until all repetitions are completed or time has elapsed. If set to **2** (the default), users are selected randomly.

.randomseed

(Defined in the Thread Control File) If configured with a non-zero integer value, causes a randomly ordered set of usernames in the range "AAAAAA" until the user name indexed by the value of the "UserCount" parameter. This allows the pseudorandom sequence of names to be repeated (up to thread ordering) for each test. If .randomseed is not specified, the current time is used.

(Optional) Configure the Sleep Time Between Policy Server Requests to Simulate a Steady Load

To simulate a steady load in which requests are sent to policy server at a constant rate, configure the following parameter in the Thread Control File.

.sleepbetweenrequests Specifies the amount of sleep time (in milliseconds) between each request to the Policy Server on each thread.

For example, if the.sleepbetweenrequests parameter is set to 5 (milliseconds), then requests are sent to the Policy Server approximately 200 times per second on each thread.

Note: The actual request rate can be influenced by the following factors: time requests take to complete, amount of CPU time that each thread gets, and external factors.

(Optional) Configure the Test Tool to Write Playback Test Results to a File in CSV Format

You can configure the Test Tool to write all playback test results to a comma-separated values (CSV) format file by setting the following system environment variable:

SMTESTCSVFILE

Specifies the pathname of the CSV file to which the Test Tool should write playback test results. Playback test results are written in comma-separated format to the specified file with a header line at the beginning. If the file already exists, the file is appended. If the Thread Control file specifies playback of multiple recordings, the results are aggregated.

Report Viewing

When you run a stress test, the Test Tool generates a report summarizing the results. This report contains the following information:

- Time the test started and finished
- Total elapsed time
- Minimum, maximum, and average request time
- Total number of requests
- Throughput
- The number of tests run and their results

The report is saved in the directory where the thread control file is located. The name of the report is the name of the thread control file with _stats appended to it. For example, the thread control file, thread.txt, yields a report named thread.txt_stats.

SiteMinder Test Tool: Cert Auth Tests

Certificate-based Authentication Tests

The CA SiteMinder® Test Tool simulates user authentication and authorization. Certificate-based authentication schemes require additional configuration.

Different certificate-generation tools sometimes affect the format of the Issuer DN and other attributes of a certificate.

For example, the Issuer DN for a certificate generated with certutil.exe on an IIS web server could use ST= to represent the state. However, the Issuer DN for a certificate generated with OpenSSL tools on an Oracle iPlanet web server could possibly use S= to represent the state.

Note: For more information about the actual values used by a specific certificate-generation tool, see the documentation provided by the vendor of your certificate-generation tool.

To test certificate-based authentication schemes, configure certificate mappings in the Policy Server to accommodate certificates created with different certificate-generation tools.

Certificate Attributes that Require Custom Mappings

Some common certificate attributes differ slightly according to the third-party tool (such as certutil.exe or OpenSSL) used to generate the certificate. Differences between the following attributes could possibly cause errors in the CA SiteMinder® Test Tool:

Email Address Represented by E or Email depending on the vendor of the certificate-generation tool.

US State Represented by S or ST depending on the vendor of the certificate-generation tool.

User ID Number Represented by UID or UserID depending on the vendor of the certificate-generation tool.

Note: For more information about the actual values used by a specific certificate-generation tool, see the documentation provided by the vendor of your certificate-generation tool.

Custom Attribute Mappings for Testing

Using the CA SiteMinder® Test Tool for a certificate authentication scheme sometimes fails, even if it works typically (through a browser and the web server). The authentication log shows that the Test Tool expects a different format of the Issuer DN than the Issuer DN format used in the certificate.

This situation occurs when the Issuer DN and other attributes differ according to the type of certificate-generation tool used. For example, the certutil.exe program on an IIS web server could possibly use ST= to abbreviate the name of the state in the Issuer DN. The OpenSSL tools on an Oracle iPlanet web server, however, could possibly use S= to abbreviate the name of the state.

Note: For more information about the actual values used by a specific certificate-generation tool, see the documentation provided by the vendor of your certificate-generation tool.

The situation is similar for the other attributes listed in [Certificate Attributes that Require Custom Mappings](#). To resolve this problem, have an administrator create mappings for each Issuer DN format in the Policy Server. Then, the Policy Sever can accept the Issuer DN formats created by different certificate-generation tools.

Issuer DN Mapping

Different certificate-generation tools (such as certutil.exe and OpenSSL) create the Issuer DN in slightly different ways. For example, one tool could possibly create an Issuer DN like the following:

CN=Personal Freemail RSA 2000.8.30, OU=Certificate Services, O=Thawte, L=Cape Town, S=Western Cape, C=ZA
Another tool could possibly create an Issuer DN like the following:

CN=Personal Freemail RSA 2000.8.30, OU=Certificate Services, O=Thawte, L=Cape Town, ST=Western Cape, C=ZA
To support multiple possibilities, have your administrator create mappings in the Policy Server for all Issuer DN formats in your environment.

Note: For more information about the actual values used by a specific certificate-generation tool, see the documentation provided by the vendor of your certificate-generation tool.

Create Custom Certificate Mappings

You can use the certificate-mapping feature of the CA SiteMinder® Policy Server to provide custom mappings for certificates.

Note: The following procedure assumes that you are creating an object. You can also copy the properties of an existing object to create an object. For more information, see Duplicate Policy Server Objects.

To create and use a custom attribute in a certificate mapping

1.Click Infrastructure, Directory.

2.Click Certification Mapping, Create Certificate Mapping.

The Create Certificate Mapping pane opens.

3.Verify that Create a new object is selected, and click OK.

Certificate mapping settings open.

Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.

4.Enter the full issuer DN in the Issuer DN field.

5.Select the Custom radio button in the Mapping group box.

The Mapping Expressions field opens.

6.Enter a custom mapping expression.

This notation is used to specify two different attributes that are acceptable for a certificate mapping.

- For Email: %{E/Email}
- For ST: %{S/ST}
- For User Id: %{UID/UserID}

7.Click Submit.

The custom mapping is saved. The Policy Server now handles requests from different types of certificate-generation tools (such as certutil.exe and OpenSSL) and the CA SiteMinder® Test tool where the Email attribute is represented differently in the issuer DN. You can use this process for any of the other attributes mentioned in [Certificate Attributes that Require Custom Mappings](#).

SiteMinder Test Tool: SSL Troubleshooting Auth Schemes

Overview

Configuring the SSL Advanced Authentication Schemes requires Web Servers to be properly configured to use SSL. Most of the problems you may encounter configuring Authentication Schemes over SSL connections are **likely to be SSL configuration issues**. Therefore, the first step in troubleshooting Authentication Schemes over SSL is to verify that SSL is properly configured and working. This is done **without the interaction** of the CA SiteMinder® Web Agent so that these components can be individually analyzed.

Determine SSL Connection Ability

The first step in troubleshooting Authentication Schemes over SSL is to verify that SSL is properly configured and working. This is done without the interaction of the CA SiteMinder® Web Agent so that these components can be individually analyzed.

To determine whether you are able to establish an SSL connection

1. Disable the CA SiteMinder® Web Agent protecting the realm for which you want to use an authentication scheme over SSL.

Note: For information about disabling a Web Agent, see the *Web Agent Configuration Guide*.

2. Using your browser, go to one of the following URLs (using a browser with a certificate):

- https://web_server_name:port/<SSL Virtual Directory> (IIS Web Servers)
- https://web_server_name:port (Apache Web Servers)

If this SSL connection is configured to require certificates, you will be prompted to select a certificate.

If you are unable to successfully establish this SSL connection, then see [SSL Configuration](#) for more information on configuring SSL. If you were able to establish this connection, but have not been successful in configuring CA SiteMinder®, see [SSL Troubleshooting](#).

SSL Configuration

It is imperative that SSL be configured and working properly before using CA SiteMinder®. In order to make an SSL connection, you must be able to trust the certificate authority of an incoming certificate. For example, if a browser presents a certificate that was signed by VeriSign, you must have a VeriSign Certificate Authority installed and trusted in the Web Server. In addition to trusting client certificates that are presented, the server itself must have a certificate to present to the clients. The clients have to trust the Certificate Authority that issued the certificate. This allows for mutual authentication. Once these certificates have been installed, you can configure the Web Server to use SSL and *require* certificates, if desired.

```
openssl s_client -connect HOSTNAME:PORT -showcerts
```

Installing the Apache Web Server Certificate

The process for installing a certificate on an Apache Web Server varies with individual configurations. Consult the documentation for [Mod_SSL](#) and OpenSSL for details about how to configure these components.

SSL Troubleshooting

The following sections detail the most common problems encountered when dealing with SSL authentication schemes.

There Was No Prompt for a Certificate

If you were not prompted for a certificate, verify that SSL is configured appropriately. If the Web Agent is installed, disable the Web Agent. The first step is to verify a simple SSL connection.

To determine whether you are able to establish an SSL connection

1. Disable the CA SiteMinder® Web Agent protecting the realm for which you want to use an authentication scheme over SSL.

Note: For information about disabling a Web Agent, see the *Web Agent Configuration Guide*.

2. Using your browser, go to one of the following URLs (using a browser with a certificate):

- https://web_server_name:port/<SSL Virtual Directory> (IIS Web Servers)
- https://web_server_name:port (Apache Web Servers)

If this SSL connection is configured to require certificates, you will be prompted to select a certificate.

After Following Previous Procedure, Still No Certificate Prompt

Perform the following five additional steps if you are still not receiving a certificate prompt.

- Verify that all Firefox browsers are configured to ask every time.
- Verify that all web servers are configured to use SSL and require certificates.
- Verify the following settings for each CA SiteMinder® Virtual Directory.
- Verify the web server certificate expiration.
- Verify browser certificate validity.

Skipped info on Netscape & info on SSL Client Certificate Authentication
See bookshelf notes for this info

1. Copy CA public key from: `openssl s_client -connect HOSTNAME:PORT -showcerts` & Save to file `ca_public_key.pem`
2. Import with Java JDK binary: `keytool -import -trustcacerts -alias root -file ca_public_key.pem -keystore yourkeystore.jks (or cacerts)`

SiteMinder Test Tool: SSL Troubleshooting Auth Schemes

Verify That All Firefox Browsers Are Configured to Ask Every Time

Firefox browsers can be configured to pass the same certificate automatically. This establishes the SSL connection using a certificate without prompting users to select a certificate.

Follow these steps:

1. In the Firefox browser, select Options from the Firefox menu.
2. Click Advanced.
3. Click the Encryption tab.
4. In the Certificates section, verify that the Ask me every time option is set.

Verify That All Web Servers Are Configured to Use SSL and Require Certificates

For IIS Web Servers

Verify that the virtual directories SMGetCredCert, SMGetCredCertOptional, SMGetCredNoCert are created and have the correct settings.

- SMGetCredCert - Require Certificates will be selected
- SMGetCredCertOptional - Accept Certificates will be selected
- SMGetCredNoCert - Do not accept certificates will be selected

Note: As part of the CA SiteMinder® SSL Authentication setup, CA SiteMinder® configures SSL virtual directories based on the type of SSL connection required by the authentication scheme.

Verify the Following Settings for each SiteMinder Virtual Directory

To verify the following settings for each CA SiteMinder® Virtual Directory

1. In the Management Console, right-click a virtual directory and select Properties.
2. Click the Directory Security tab.
3. Click Edit Secure Communications.

For Apache Web Servers

In the httpd.conf file, be sure to set SSLVerifyClient as follows:

- For **Basic over SSL: SSLVerifyClient none**
- For Certificate or Basic: SSLVerifyClient optional
- For Certificate/Certificate and Basic: SSLVerifyClient require

Note: For Apache Web servers where Certificates are required or optional, the **"SSL Verify Depth 10"** line in the httpd.conf file must be uncommented.

```
openssl s_client -connect HOSTNAME:PORT -showcerts
```

SiteMinder Test Tool: SSL Troubleshooting Auth Schemes

Check the Web Server's Certificate Expiration

IIS Servers

1. In the Management Console, right-click the Web Server and select Properties.
2. Click the Directory Security tab.
3. In the Secure Communications panel, click Key Manager.
4. Select a key to view its properties and verify that the key has not expired.
5. If you need to make any changes, restart the Web Server.

Apache Servers

If an Apache Web Server certificate expires, you will receive an error messages at server startup that indicates the certificate has expired.

Verify Browser Certificate Validity

A missing certificate or an invalid certificate can prevent you from receiving a certificate prompt. Open your Web browser and verify the validity of the browser certificate.

Note: For more information about viewing certificate information, see your vendor-specific documentation.

After Certificate Prompt, Authentication Failure Received

Apache Web Servers

- Verify that the SSL Web Server contains the **certificate authority** of the certificate supplied.
- Verify that the SSL Web Server **Trusts the certificate authority** of that certificate.
- Ensure the **SSL Verify Depth 10** is uncommented.

IIS Web Servers

Verify that the certificate is listed and that it is valid. If it is not present or is not valid, install a new certificate. If you are able to get to the destination directory, then certificates are installed correctly.

Verify Correct Policy Server and Web Agent Configuration

After completing the steps in the previous topic based on your specific web server, verify your policy server and web agent configuration.

To verify correct policy server and web agent configuration

1. Check that the Policy Server is created correctly.
2. Check that the Web Agent contains the correct Policy Server information.
3. Verify that the Web Agent is enabled.
4. Restart the Web Agent and Policy Server.

SiteMinder Policy Should Allow Access, but SSL-Authentication Failed Message Received

In this situation, there is a Policy that is being called, but the user is incorrectly being denied access. This can result from a number of configuration errors. Common errors include:

- The SSL Server is not configured to Require Client Certificates. Therefore, the client is not passing a certificate; thereby disabling CA SiteMinder® authentication process. You can verify this is the situation by enabling the logging option in the Web Agent. The log should indicate that the user is unknown. To correct this problem, turn on Require Certificates in the SSL Web Server.
- The Policy was not created properly. Check the Policy's users and be sure that the selection is correct.
- For Apache Web server, ensure the SSL Verify Depth is set properly and uncommented.

Error Not Found Message Received

This is generally caused from the Authentication Scheme Parameter being configured improperly. The redirect is not configured properly so the Web Server is unable to find the SSL Web Agent component.

More information:

[Authentication Schemes](#)

Running Certificate or Basic but Cannot Enter Basic credentials.

On Netscape Web Servers, the *Certificate or Basic* scheme requires the Web Server to have encryption turned on, but does not require certificates. Be sure that in the Encryption Preferences section of the Netscape Server Administration, the **Require Certificate setting is set to No**.

```
openssl s_client --connect HOSTNAME:PORT -showcerts
```